Smart Ways to Monitor and Evaluate the ESF: How to Gain Access to Administrative Data while Complying with Data Protection Rules

Final Report

Written by:
Emmanuel Hassan
Per Lundberg
Ela Omersa
Caro Robson
Flore Gustave
Costanza Pagnini
Massimo Marziali
September - 2023

EUROPEAN COMMISSION

Directorate-General for Employment, Social Affairs and Inclusion
Directorate G — Funds, Programming and Implementation
Unit G5 — Better Regulation

Contact: Linda Adamaite

E-mail: EMPL-G5-UNIT@@*ec.europa.eu*
Linda.Adamaite@ec.europa.eu

European Commission
B-1049 Brussels

Smart ways to monitor and evaluate the ESF: How to Gain Access to Administrative Data while Complying with Data Protection Rules

Final Report

Directorate-General for Employment, Social Affairs and Inclusion

2023

Manuscript completed in September 2023

Luxembourg: Publications Office of the European Union, 2023

PDF ISBN 978-92-68-07593-7 doi:10.2767/580113 KE-04-23-884-EN-N

Table of Contents

List of boxes

List of figures

List of tables

Executive summary

The European Social Fund Plus (ESF+) is a publicly funded programme, the oldest and one of the largest European Structural and Investment Funds. In order to ensure accountability and performance, monitoring and evaluation are key elements. For that, accurate, statistically robust data on (ESF/ESF+) participants (and organisations) are necessary. As much of these data often needs to be collected in a personally identifiable form (whether from participants themselves or from administrative records), its use for monitoring and evaluation must comply with data protection rules at EU and Member State level. The use of administrative registers as a means of collecting monitoring and evaluation data can be more effective and efficient than relying solely on questionnaires. However, access to these data can be challenging due to either bureaucratic or legal requirements related to the protection of personal data.

The purpose of this study was to assess the legal and practical challenges in accessing and re-using administrative data for the purposes of monitoring and evaluation of ESF and ESF+ programmes. In order to facilitate the monitoring and evaluation of ESF+, the study also assessed how to facilitate access to administrative data, with the aim of providing guidance to managing authorities on how to process personal data, including administrative data, while complying with data protection rules.

In order to draw the necessary conclusions and make recommendations, the study has:

- Described the legal framework at EU level with implications for the monitoring and evaluation of ESF+.
- Provided an outline description of national legal frameworks to gain futher insights into how a selection of nine Member States (Austria, Germany, Spain, France, Ireland, Italy, Poland, Romania, and Sweden) apply and supplement the EU legal framework.
- Assessed examples of dataset and sector-specific legislation from three selected Member States (Austria, Spain, and Romania) to gain a deeper insight into the diversity and multiplicity of national legislation to be considered for datasets that are held by public authorities.
- Analysed data protection aspects relevant to to the monitoring and evaluation of the ESF+, including the relevant legal bases, provisions and national practices relevant to the reuse of data, consent, special categories of personal data, transmission of data, data linking, data storage, and informing data subjects.
- Developed models of accessing administrated data in nine Member States, including a deeper review of three Member States (Austria, Spain and Italy) and related legal obligations and conditions to access these data.
- Conducted 50 stakeholder interviews, complemented by several rounds of follow-up questions, with a wide range of relevant stakeholders in nine Member States to identify practices, challenges, and possible solutions to the processing of data for the purpose of implementing, monitoring, and evaluating ESF/ESF+ Projects. The study also organised a Focus Group with participants of key stakeholders from 13 Member States to assess the main issues at stake and to jointly explore possible solutions.

The conclusions of the legal research and stakeholder consultations have mainly been used to identify challenges related to the processing of administrative data for ESF/ESF+ monitoring and evaluation, and to develop recommendations to overcome those challenges. These challenges and recommendations are presented in the last section of this executive summary as well as in Chapter 7 of this report. However, there are a number of conclusions introduced below that are relevant to highlight as a result of the legal research and stakeholder consultations, involving the most appropriate legal bases and Member State models of access to administrative data.

Appropriate legal bases for the processing of administrative data

Sources and case law at EU level show that although several legal bases in the GDPR[1] can be used to legitimise the processing of (including access to) administrative data of participants and non-participants, the most appropriate legal bases appear to be:

- fulfilment of a legal obligation[2] and
- the performance of a task carried out in the public interest[3].

Both of these legal bases leave some discretion to Member States in a sense that national GDPR-implementing laws may contain specific provisions to adapt the application of the GDPR rules, as stated in Article 6(2) and (3) GDPR.

Among the nine Member States sampled for this study, consent as a legal basis has been the most common practice so far when collecting personal data directly from ESF participants. However, using consent as a legal basis may involve a heavy administrative burden, and the legal analysis in Section 5.3 of this study shows that using consent as a legal basis is often not suitable, especially not when personal data are collected by a public authority.

Another challenge related to consent is that if problems in its validity occur, national authorities cannot migrate from consent to another legal basis retroactively in order to justify processing. Only in certain cases can consent be replaced with another legal basis, which better reflects the situation, i.e., in case of withdrawal of a consent or processing for a new/additional purpose. However, any change must be notified to data subjects in accordance with the information requirements in Articles 13 and 14 GDPR.

Moreover, relying on explicit consent to lift the ban of processing special categories of personal data is especially challenging. Instead, the use of exceptions in Article 9(2)(g) on the processing for reasons of substantial public interest, Article 9(2)(h) on the processing for reasons of medicinal purposes, or Article 9(2)(i) on the processing of data for reasons of public interest in the area of public health is more suitable.

There are three possibilities for the reuse of administrative data, namely (i) if the purpose of the reuse of administrative data is compatible with the initial purpose of the processing of these administrative data; (ii) if a legal basis for the reuse of administrative data exists in national law; or (iii) if the reuse is carried out for the purpose of scientific research. With regard to the latter, although there are interpretations and arguments both for and against considering that evaluations carried out or commissioned by the managing authorities are considered as scientific research, it can be argued based on GDPR Article 5(1)(b) in

[1] Article 6, GDPR.

[2] Article 6(1)(c), GDPR.

[3] Article 6(1)(e), GDPR.

connection with Article 89(1), that evaluations under certain circumstances can qualify as such research.

Member State models of access to administrative data

Based on interviews and desk research, most country models to access and link administrative data for ESF/ESF+ monitoring and evaluation are decentralised across different institutions and levels of government. Sweden is the only Member State out of the nine covered in this study that has centralised its model of access to administrative data for ESF/ESF+ monitoring and evaluation. The model of access to administrative data in Sweden could be described as centralised and harmonised as all data processing and linking is centralised to Statistics Sweden. Models of access to administrative data in all other eight Member States (Austria, Germany, Spain, France, Ireland, Italy, Poland, and Romania) are decentralised. In these Member States, there may be central databases that store data that are collected directly from the ESF/ESF+ participants and the managing authorities may play a coordinating role. However pre-existing administrative data that are used to complement and link data for monitoring and evaluation are neither coordinated nor processed centrally.

Evaluators can also access administrative data without the need to inform the managing authority. For example, in Spain, France, Poland, and Romania, administrative data must be accessed from each individual institution that hosts these data, and the processes to do so may vary depending on the institution and region. In Ireland, there are attempts to harmonise datasets such as via the Jobseekers Longitudinal Dataset (JLD), and there are examples of coherent models used by individual intermediary bodies with access to their own administrative data. However, there is no nation-wide model, and the managing authority is not involved in the process. Lastly, whilst the Austrian managing authority manages a central database containing participants' data collected for ESF/ESF+ purposes, access to administrative data for ESF/ESF+ purposes is not centralised nor harmonised.

Decentralised data processing models may come with challenges when it comes to effectiveness and efficiency in the processing of administrative data for ESF/ESF+ monitoring and evaluation. These challenges are among other challenges identified in this study introduced in the next section, together with recommendations developed to overcome these challenges.

Main challenges identified and recommendations to overcome these challenges

Challenges and recommendations related to the knowledge and choice of the most appropriate legal basis

One challenge detected in this study is that it may be difficult for managing authorities, beneficiaries, and evaluators to navigate between the possible legal bases and to assess which one is the most appropriate, effective, and efficient to use for data processing in the monitoring and evaluation of the ESF+. Therefore, the study recommends that:

- Member States and ESF+ managing authorities should consult their national Data Protection Authority (DPA) on the applicable data protection rules, including the legal basis for processing personal data for the purpose of ESF+ evaluation and monitoring, if there is any doubt regarding the available options under national or Union law. Where a gap in legislation is identified, Member States should consider possible legislative initiatives to provide clear data protection rules, including a legal

basis for reusing administrative data for the purpose of ESF+ monitoring and evaluation.

Challenges and recommendations related to the reuse of administrative data and/or the further use of data for scientific research

Administrative data in existing national databases can only be further processed for ESF+ monitoring and evaluation purposes if the necessary conditions are met (e.g., if a further use is compatible with the original purpose, including the case where processing for ESF+ purposes could be considered as scientific research) or if there is a specific legal base for reuse. As described above, in the case of evaluations, there are arguments both for considering that evaluations carried out or commissioned by the managing authorities can be considered as scientific research and for considering that they cannot, also depending on the scope and quality of the methodology of the evaluations in question. Therefore, the study recommends that:

- Member States should provide a clear legal basis for the reuse of administrative data at national level.
- National DPAs should provide opinions/guidelines on when the reuse of administrative data can be considered as processing for 'compatible purposes', on the possibility to further process personal data for scientific research purposes, when ESF+ evaluation can be considered as 'scientific research', as well as on the appropriate safeguards for data subjects.
- National administrative authorities should conclude data sharing agreements to facilitate the exchange of administrative data for ESF+ purposes.

Challenges and recommendations related to the processing of special categories of personal data

The processing of special categories of personal data requires both a valid legal basis and an exemption to lift the prohibition on the processing of special categories of personal data. As the processing of special categories of personal data represents a greater interference with the rights of data subjects, the GDPR requires that specific safeguards are provided by law to protect individuals' personal data. Stakeholder interviews showed that for the ESF 2014-2020 programming period, beneficiaries in most of the Member States covered by this study collected special categories of personal data. However, in some Member States it was not always possible to process those data.Therefore, the study recommends that:

- When processing special categories of personal data, the principle of data minimisation should apply, including through anonymisation.
- Member States ensure that there is a legal basis for the processing as well as an applicable provision to lift the prohibition to process special categories of personal data and that the appropriate safeguards required by national law are in place.
- Managing authorities, if necessary, seek advice on applicable rules and appropriate safeguards from data protection experts (national DPAs, DPOs, or consultants).
- Alternative methods are used to process special categories of personal data (e.g., informed estimates).

Challenges and recommendations related to the lack of understanding and/or awareness of the national legal framework for the processing of administrative data

To understand how personal data should be processed in Member States, several pieces of legislation need to be taken into account. The EU Charter and the ECHR must be respected, and any processing activity must also comply with the provisions of the GDPR, the CPR 2021 and the ESF+ Regulation. In addition, national legislation must also be complied with, and here, too, several layers of instruments must be taken into account. The processing of personal data must comply with the requirements of national constitutions, national legislation supplementing the GDPR, national (or even regional) sectoral and dataset-specific legislation, as well as sector-specific data soft law.

While general rules are set out in overarching legal instruments such as the GDPR, these do not always provide detailed rules on how to deal with each specific type of data, and therefore often allow Member States to adapt these rules or provide for more specific rules in light of the needs of processing operations in specific sectors. Certain legal bases of the GDPR[4] leave Member States the discretion to further regulate certain aspects of data processing in their national legislation. In the absence of clear guidance, actors involved in the monitoring and evaluation of the ESF+ may therefore face difficulties in understanding which rules apply and what possibilities they may entail. Therefore, the study recommends stakeholders to:

- Consider the possibilities, rather than limitations, provided by national legislation in combination with EU law to facilitate the processing of administrative data in an ESF+ context.
- Seek advice, guidance, and/or participate in training of data protection experts (national DPAs, DPOs, or consultants), where appropriate together with other data protection specialists, in order to better understand the applicable legal framework and requirements that apply to the processing of administrative data for the purpose of monitoring and evaluation of the ESF+.
- Carry out, where appropriate, data protection impact assessments (DPIAs) for new projects and encourage the exchange of promising examples or templates for such assessments.

Challenges and recommendations related to low levels of interoperability of national registers and the level of centralisation of data processing

A common challenge in accessing administrative data is that the data relevant for ESF/ESF+ monitoring or evaluation are held by different institutions and/or at different administrative levels. These data may in some cases be hard to compare, also with ESF+ indicators, partly due to varying definitions of data. Thus, decentralised hosting of data may lead to issues related to interoperability of national registers that are relevant for monitoring or evaluating the ESF+. In addition, different data sets may be subject to different data protection rules and different consent requirements. Therefore, the study recommends to:

- Consider the possibility of centralising data processing, including the hosting of data relevant for the monitoring and evaluation of the ESF+.

[4] Article 6(1)(c) and (e), GDPR.

- Promote the centralisation of the management and coordination of access to administrative data for the purposes of ESF+ monitoring and evaluation.
- Consider the use of pseudonymisation as a technique to mitigate data protection risks.

Challenges and recommendations related to unnecessary costs, delays and data incompatibility

Obtaining access to administrative data can be time-consuming and there may be a long waiting period after a request has been made. There may also be financial costs associated with accessing administrative data, as organisations, especially external evaluators, may need to purchase data from data holders. In addition, data may be defined differently by data holders and data may not be comparable between databases within Member States. Therefore, the study recommends:

- To plan well in advance what administrative data will be needed to complement or replace direct data collection for ESF+ monitoring and evaluation.
- Managing authorities should coordinate planning with administrative data holders who may know what data are available.

Challenges and recommendations related to a lack of mutual learning between Member States on data protection-related issues concerning access to administrative data for ESF/ESF+ purposes

There are practices that can be applied to overcome the challenges of accessing administrative data. Several Illustrative examples of good practice in accessing administrative data for ESF+ monitoring and evaluation purposes were identified during the interviews in this study. Therefore, the study recommends:

- Member States and managing authorities to exchange good practices on access to administrative data for ESF/ESF+ purposes.
- Relevant EU authorities to continue to organise contact points where relevant stakeholders from Member States can meet and network. When relevant, involve data protection authorities in such fora.
- The development of a practical document and/or handbook for Member States and/or competent authorities.

Résumé

Le Fonds social européen Plus (FSE+) est un programme financé par des fonds publics, le plus ancien et l'un des plus importants Fonds structurels et d'investissement européens. Pour garantir la responsabilité et la performance, le suivi et l'évaluation sont des éléments clés. Pour ce faire, il est nécessaire de disposer de données précises et statistiquement fiables sur les participants (et les organisations) du FSE/FSE+. Étant donné qu'une grande partie de ces données doit souvent être collectée sous une forme personnellement identifiable (que ce soit auprès des participants eux-mêmes ou à partir de registres administratifs), leur utilisation à des fins de suivi et d'évaluation doit être conforme aux règles de protection des données en vigueur au niveau de l'UE et des États membres. L'utilisation de registres administratifs comme moyen de collecte de données de suivi et d'évaluation peut s'avérer plus efficace et plus rentable que le recours exclusif à des questionnaires. Toutefois, l'accès à ces données peut s'avérer difficile en raison d'exigences bureaucratiques ou juridiques liées à la protection des données à caractère personnel.

L'objectif de cette étude était d'évaluer les défis juridiques et pratiques liés à l'accès et à la réutilisation des données administratives à des fins de suivi et d'évaluation des programmes du FSE et du FSE+. Afin de faciliter le suivi et l'évaluation du FSE+, l'étude a également évalué comment faciliter l'accès aux données administratives, dans le but de fournir des orientations aux autorités de gestion sur la manière de traiter les données à caractère personnel, y compris les données administratives, tout en respectant les règles de protection des données.

Afin de tirer les conclusions nécessaires et de formuler des recommandations, l'étude a :

- Présenté le cadre juridique au niveau de l'UE et analysé les conséquences pour le suivi et l'évaluation du FSE+.

- Fourni une description succinte des cadres juridiques nationaux afin de mieux comprendre comment certains États membres (Autriche, Allemagne, Espagne, France, Irlande, Italie, Pologne, Roumanie et Suède) appliquent et complètent le cadre juridique de l'UE.

- Evalué des exemples de législations spécifiques à des ensembles de données et à des secteurs dans trois États membres sélectionnés (Autriche, Espagne et Roumanie) afin de mieux comprendre la diversité et la multiplicité des législations nationales à prendre en compte pour les ensembles de données détenus par les autorités publiques.

- Analysé des aspects de la protection des données pertinents pour le suivi et l'évaluation du FSE+, y compris les bases juridiques adéquates, les dispositions et les pratiques nationales relatives à la réutilisation des données, au consentement, aux catégories spéciales de données à caractère personnel, à la transmission des données, à l'interconnexion des données, au stockage des données et à l'information des personnes concernées.

- Elaboré des modèles d'accès aux données administratives dans neuf États membres, y compris un examen plus approfondi de trois États membres (Autriche, Espagne et Italie) et des obligations légales et conditions d'accès à ces données.

- 50 entretiens, complétés par plusieurs séries de questions, avec un large éventail de parties prenantes dans neuf États membres afin d'identifier les pratiques, les défis et les solutions possibles au traitement des données dans le but de mettre en

œuvre, de suivre et d'évaluer les projets du FSE/FSE+. L'étude a également organisé un groupe de discussion avec des participants des principales parties prenantes de 13 États membres afin d'évaluer les principaux enjeux et d'explorer conjointement les solutions possibles.

Les conclusions de la recherche juridique et des consultations des parties prenantes ont principalement été utilisées pour identifier les défis liés au traitement des données administratives pour le suivi et l'évaluation du FSE/FSE+, et pour développer des recommandations afin de surmonter ces défis. Ces défis et recommandations sont présentés dans la dernière section de cette synthèse ainsi qu'au chapitre 7 de ce rapport. Cependant, un certain nombre de conclusions présentées ci-dessous sont pertinentes pour souligner le résultat de la recherche juridique et des consultations des parties prenantes, impliquant les bases juridiques les plus appropriées et les modèles d'accès aux données administratives dans les États membres.

Bases juridiques appropriées pour le traitement des données administratives

Les sources et la jurisprudence au niveau de l'UE montrent que, bien que plusieurs bases juridiques du règlement général sur la protection des données (RGPD)[5] puissent être utilisées pour légitimer le traitement (y compris l'accès) des données administratives des participants et des non-participants, les bases juridiques les plus appropriées semblent être les suivantes :

- le respect d'une obligation légale[6] et
- l'exécution d'une mission d'intérêt public[7] .

Ces deux bases juridiques laissent une certaine marge de manœuvre aux États membres en ce sens que les lois nationales de mise en œuvre du RGPD peuvent contenir des dispositions spécifiques pour adapter l'application des règles du RGPD, comme le prévoit l'article 6, paragraphes 2 et 3, du RGPD.

Parmi les neuf États membres échantillonnés pour cette étude, le consentement comme base juridique a été la pratique la plus courante jusqu'à présent lors de la collecte de données à caractère personnel directement auprès des participants au FSE. Toutefois, l'utilisation du consentement comme base juridique peut entraîner une lourde charge administrative, et l'analyse juridique de la section 5.3 de la présente étude montre que l'utilisation du consentement comme base juridique n'est souvent pas appropriée, en particulier lorsque les données à caractère personnel sont collectées par une autorité publique.

Un autre problème lié au consentement est qu'en cas de problèmes de validité, les autorités nationales ne peuvent pas passer rétroactivement du consentement à une autre base juridique afin de justifier le traitement. Ce n'est que dans certains cas que le consentement peut être remplacé par une autre base juridique, qui reflète mieux la situation, c'est-à-dire en cas de retrait du consentement ou de traitement pour une finalité nouvelle ou supplémentaire. Toutefois, tout changement doit être notifié aux personnes concernées conformément aux exigences en matière d'information prévues aux articles 13 et 14 du RGPD.

[5] Article 6, RGPD.

[6] Article 6, paragraphe 1, point c), du RGPD.

[7] Article 6, paragraphe 1, point e), du RGPD.

En outre, il est particulièrement difficile de s'appuyer sur le consentement explicite pour lever l'interdiction de traiter des catégories particulières de données à caractère personnel. Le recours aux exceptions prévues à l'article 9, paragraphe 2, point g), concernant le traitement pour des raisons d'intérêt public majeur, à l'article 9, paragraphe 2, point h), concernant le traitement à des fins médicales, ou à l'article 9, paragraphe 2, point i), concernant le traitement de données pour des raisons d'intérêt public dans le domaine de la santé publique, est plus approprié.

Il existe trois possibilités de réutilisation des données administratives, à savoir (i) si la finalité de la réutilisation des données administratives est compatible avec la finalité initiale du traitement de ces données administratives ; (ii) si une base juridique pour la réutilisation des données administratives existe dans le droit national ; ou (iii) si la réutilisation est effectuée à des fins de recherche scientifique. En ce qui concerne ce dernier point, bien qu'il existe des interprétations et des arguments à la fois pour et contre le fait de considérer les évaluations réalisées ou commandées par les autorités de gestion comme de la recherche scientifique, on peut affirmer, sur la base de l'article 5, paragraphe 1, point b), du RGPD, en liaison avec l'article 89, paragraphe 1, que les évaluations peuvent, dans certaines circonstances, être considérées comme de la recherche scientifique.

Modèles d'accès aux données administratives dans les États membres

D'après les entretiens et les recherches documentaires, la plupart des modèles nationaux d'accès et de liaison des données administratives pour le suivi et l'évaluation du FSE/FSE+ sont décentralisés entre les différentes institutions et les différents niveaux de gouvernement. La Suède est le seul État membre, parmi les neuf couverts par cette étude, à avoir centralisé son modèle d'accès aux données administratives pour le suivi et l'évaluation du FSE/FSE+. Le modèle d'accès aux données administratives en Suède pourrait être décrit comme centralisé et harmonisé, car tous les traitements de données et les liens sont centralisés à Statistics Sweden. Les modèles d'accès aux données administratives dans les huit autres États membres (Autriche, Allemagne, Espagne, France, Irlande, Italie, Pologne et Roumanie) sont décentralisés. Dans ces États membres, il peut y avoir des bases de données centrales qui stockent les données collectées directement auprès des participants au FSE/FSE+ et les autorités de gestion peuvent jouer un rôle de coordination. Cependant, les données administratives préexistantes qui sont utilisées pour compléter et relier les données pour le suivi et l'évaluation ne sont ni coordonnées ni traitées de manière centralisée.

Les évaluateurs peuvent également accéder aux données administratives sans avoir à en informer l'autorité de gestion. Par exemple, en Espagne, en France, en Pologne et en Roumanie, les données administratives doivent être consultées auprès de chaque institution qui héberge ces données, et les procédures à suivre peuvent varier en fonction de l'institution et de la région. En Irlande, il existe des tentatives d'harmonisation des ensembles de données, par exemple via le Jobseekers Longitudinal Dataset (JLD), et il existe des exemples de modèles cohérents utilisés par des organismes intermédiaires individuels ayant accès à leurs propres données administratives. Cependant, il n'existe pas de modèle national et l'autorité de gestion n'est pas impliquée dans le processus. Enfin, si l'autorité de gestion autrichienne gère une base de données centrale contenant les données des participants collectées aux fins du FSE/FSE+, l'accès aux données administratives aux fins du FSE/FSE+ n'est ni centralisé ni harmonisé.

Les modèles décentralisés de traitement des données peuvent présenter des difficultés en termes d'efficacité et d'efficience dans le traitement des données administratives pour le suivi et l'évaluation du FSE/FSE+. Ces défis, parmi d'autres identifiés dans cette étude, sont présentés dans la section suivante, ainsi que les recommandations élaborées pour surmonter ces défis.

Principaux défis identifiés et recommandations pour les surmonter

Défis et recommandations liés à la connaissance et au choix de la base juridique la plus appropriée

L'un des défis détectés dans cette étude est qu'il peut être difficile pour les autorités de gestion, les bénéficiaires et les évaluateurs de naviguer entre les bases juridiques possibles et d'évaluer laquelle est la plus appropriée, la plus efficace et la plus efficiente à utiliser pour le traitement des données dans le cadre du suivi et de l'évaluation du FSE+. Par conséquent, l'étude recommande ce qui suit

- Les États membres et les autorités de gestion du FSE+ devraient consulter leur autorité nationale de protection des données sur les règles applicables en matière de protection des données, y compris la base juridique pour le traitement des données à caractère personnel aux fins de l'évaluation et du suivi du FSE+, en cas de doute concernant les options disponibles en vertu du droit national ou de l'Union. Lorsqu'une lacune dans la législation est identifiée, les États membres devraient envisager d'éventuelles initiatives législatives afin de fournir des règles claires en matière de protection des données, y compris une base juridique pour la réutilisation des données administratives aux fins du suivi et de l'évaluation du FSE+.

Défis et recommandations liés à la réutilisation des données administratives et/ou à l'utilisation ultérieure des données pour la recherche scientifique

Les données administratives contenues dans les bases de données nationales existantes ne peuvent être traitées ultérieurement à des fins de suivi et d'évaluation du FSE+ que si les conditions nécessaires sont remplies (par exemple, si une utilisation ultérieure est compatible avec l'objectif initial, y compris le cas où le traitement à des fins du FSE+ pourrait être considéré comme de la recherche scientifique) ou s'il existe une base juridique spécifique pour la réutilisation. Comme décrit ci-dessus, dans le cas des évaluations, il existe des arguments à la fois pour considérer que les évaluations réalisées ou commandées par les autorités de gestion peuvent être considérées comme de la recherche scientifique et pour considérer qu'elles ne peuvent pas l'être, en fonction également de la portée et de la qualité de la méthodologie des évaluations en question. Par conséquent, l'étude recommande ce qui suit :

- Les États membres devraient fournir une base juridique claire pour la réutilisation des données administratives au niveau national.

- Les autorités nationales de protection des données devraient fournir des avis/orientations sur les cas où la réutilisation de données administratives peut être considérée comme un traitement à des "fins compatibles", sur la possibilité de traiter ultérieurement des données à caractère personnel à des fins de recherche scientifique, sur les cas où l'évaluation du FSE+ peut être considérée comme de la "recherche scientifique", ainsi que sur les garanties appropriées pour les personnes concernées.

- Les autorités administratives nationales devraient conclure des accords de partage de données afin de faciliter l'échange de données administratives aux fins du FSE+.

Défis et recommandations liés au traitement de catégories particulières de données à caractère personnel

Le traitement de catégories particulières de données à caractère personnel nécessite à la fois une base juridique valable et une dérogation pour lever l'interdiction de traitement de catégories particulières de données à caractère personnel. Étant donné que le traitement de catégories spéciales de données à caractère personnel représente une ingérence plus importante dans les droits des personnes concernées, le RGPD exige que des garanties spécifiques soient prévues par la loi pour protéger les données à caractère personnel des individus. Les entretiens avec les parties prenantes ont montré que pour la période de programmation du FSE 2014-2020, les bénéficiaires de la plupart des États membres couverts par cette étude ont collecté des catégories spéciales de données à caractère personnel. Toutefois, dans certains États membres, il n'a pas toujours été possible de traiter ces données . Par conséquent, l'étude recommande ce qui suit :

- Lors du traitement de catégories particulières de données à caractère personnel, le principe de minimisation des données devrait s'appliquer, y compris par le biais de l'anonymisation.

- Les États membres veillent à ce qu'il existe une base juridique pour le traitement ainsi qu'une dérogation applicable pour lever l'interdiction de traiter des catégories particulières de données à caractère personnel et à ce que les garanties appropriées requises par le droit national soient en place.

- Les autorités de gestion demandent, si nécessaire, des conseils sur les règles applicables et les garanties appropriées à des experts en protection des données (autorités nationales de protection des données, délégués à la protection des données ou consultants).

- Des méthodes alternatives sont utilisées pour traiter des catégories spéciales de données à caractère personnel (par exemple, des estimations solidement étayées fournies par les bénéficiaires).

Défis et recommandations liés au manque de compréhension et/ou de connaissance du cadre juridique national pour le traitement des données administratives

Pour comprendre comment les données à caractère personnel doivent être traitées dans les États membres, il convient de tenir compte de plusieurs textes législatifs. La Charte de l'UE et la CEDH doivent être respectées, et toute activité de traitement doit également être conforme aux dispositions du RGPD, du RDC 2021 et du règlement FSE+. En outre, la législation nationale doit également être respectée et, là aussi, plusieurs niveaux d'instruments doivent être pris en compte. Le traitement des données à caractère personnel doit être conforme aux exigences des constitutions nationales, de la législation nationale complétant le RGPD, de la législation nationale (ou même régionale) sectorielle et spécifique aux ensembles de données, ainsi que de la loi sectorielle sur les données non contraignantes.

Si des règles générales sont énoncées dans des instruments juridiques globaux tels que le RGPD, elles ne fournissent pas toujours des règles détaillées sur la manière de traiter chaque type spécifique de données, et permettent donc souvent aux États membres d'adapter ces règles ou de prévoir des règles plus spécifiques à la lumière des besoins des opérations de traitement dans des secteurs spécifiques. Certaines bases juridiques du

RGPD[8] laissent aux États membres la possibilité de réglementer davantage certains aspects du traitement des données dans leur législation nationale. En l'absence d'orientations claires, les acteurs impliqués dans le suivi et l'évaluation du FSE+ peuvent donc avoir des difficultés à comprendre quelles règles s'appliquent et quelles possibilités elles peuvent impliquer. Par conséquent, l'étude recommande aux parties prenantes de

- Envisager les possibilités, plutôt que les limites, offertes par la législation nationale en combinaison avec le droit communautaire pour faciliter le traitement des données administratives dans le contexte du FSE+.

- Demander des conseils, des orientations et/ou participer à la formation d'experts en protection des données (DPA nationales, DPD ou consultants), le cas échéant avec d'autres spécialistes de la protection des données, afin de mieux comprendre le cadre juridique applicable et les exigences qui s'appliquent au traitement des données administratives aux fins du suivi et de l'évaluation du FSE+.

- Réaliser, le cas échéant, des évaluations de l'impact sur la protection des données (DPIA) pour les nouveaux projets et encourager l'échange d'exemples prometteurs ou de modèles pour de telles évaluations.

Défis et recommandations liés aux faibles niveaux d'interopérabilité des registres nationaux et au niveau de centralisation du traitement des données

L'accès aux données administratives se heurte souvent au fait que les données pertinentes pour le suivi ou l'évaluation du FSE/FSE+ sont détenues par différentes institutions et/ou à différents niveaux administratifs. Dans certains cas, ces données peuvent être difficiles à comparer, y compris avec les indicateurs du FSE+, en partie à cause de définitions différentes des données. Ainsi, l'hébergement décentralisé des données peut entraîner des problèmes liés à l'interopérabilité des registres nationaux qui sont pertinents pour le suivi ou l'évaluation du FSE+. En outre, les différents ensembles de données peuvent être soumis à des règles différentes en matière de protection des données et à des exigences différentes en matière de consentement. Par conséquent, l'étude recommande de :

- Envisager la possibilité de centraliser le traitement des données, y compris l'hébergement des données pertinentes pour le suivi et l'évaluation du FSE+.

- Promouvoir la centralisation de la gestion et de la coordination de l'accès aux données administratives aux fins du suivi et de l'évaluation du FSE+.

- Envisager l'utilisation de la pseudonymisation comme technique pour atténuer les risques liés à la protection des données.

Défis et recommandations concernant les coûts inutiles, les retards et l'incompatibilité des données

Obtenir l'accès aux données administratives peut prendre du temps et il peut y avoir une longue période d'attente après une demande. L'accès aux données administratives peut également entraîner des coûts financiers, car les organisations, en particulier les évaluateurs externes, peuvent avoir besoin d'acheter des données auprès des détenteurs de données. En outre, les données peuvent être définies différemment par les détenteurs

[8] Article 6, paragraphe 1, points c) et e), du RGPD.

de données et les données peuvent ne pas être comparables entre les bases de données au sein des États membres. C'est pourquoi l'étude recommande ce qui suit

- Planifier longtemps à l'avance les données administratives qui seront nécessaires pour compléter ou remplacer la collecte directe de données pour le suivi et l'évaluation du FSE+.

- Les autorités de gestion doivent coordonner la planification avec les détenteurs de données administratives qui peuvent connaître les données disponibles.

Défis et recommandations liés au manque d'apprentissage mutuel entre les États membres sur les questions relatives à la protection des données concernant l'accès aux données administratives aux fins du FSE/FSE+.

Certaines pratiques peuvent être appliquées pour surmonter les difficultés liées à l'accès aux données administratives. Plusieurs exemples de bonnes pratiques en matière d'accès aux données administratives à des fins de suivi et d'évaluation du FSE+ ont été identifiés au cours des entretiens menés dans le cadre de cette étude. Par conséquent, l'étude recommande ce qui suit

- Les États membres et les autorités de gestion doivent échanger des bonnes pratiques sur l'accès aux données administratives aux fins du FSE/FSE+.

- Les autorités compétentes de l'UE doivent continuer à organiser des points de contact où les parties prenantes des États membres peuvent se rencontrer et travailler en réseau. Le cas échéant, impliquer les autorités chargées de la protection des données dans ces forums.

- L'élaboration d'un document pratique et/ou d'un manuel à l'intention des États membres et/ou des autorités compétentes.

Zusammenfassung

Der Europäische Sozialfonds Plus (ESF+) ist ein öffentlich finanziertes Programm, das älteste und eines der größten europäischen Struktur- und Investitionsfonds. Um Verantwortlichkeit und Effizienz zu gewährleisten, sind Monitoring und Evaluierung von zentraler Bedeutung. Dafür sind genaue, statistisch solide Daten über (ESF/ESF+) Teilnehmer (und Organisationen) erforderlich. Da viele dieser Daten häufig in persönlich identifizierbarer Form erhoben werden müssen (entweder von den Teilnehmern selbst oder aus administrativen Unterlagen), muss ihre Verwendung für Monitoring und Evaluierung den Datenschutzbestimmungen auf EU- und Mitgliedstaatsebene entsprechen. Die Verwendung von administrativen Registern als Mittel zur Erhebung von Monitoring- und Evaluierungsdaten kann effektiver und effizienter sein als die ausschließliche Verwendung von Fragebögen. Der Zugang zu diesen Daten kann jedoch aufgrund bürokratischer oder rechtlicher Anforderungen in Bezug auf den Schutz personenbezogener Daten eine Herausforderung darstellen.

Ziel dieser Studie war es, die rechtlichen und praktischen Herausforderungen beim Zugang zu Verwaltungsdaten und deren Weiterverwendung für die Monitoring- und Evaluierungszwecke von ESF- und ESF+-Programmen zu bewerten. Um die Monitoring- und Evaluierungsmaßnahmen von ESF+ zu erleichtern, wurde in der Studie auch untersucht, wie der Zugang zu Verwaltungsdaten erleichtert werden kann, mit dem Ziel, den Verwaltungsbehörden eine Anleitung zu geben, wie personenbezogene Daten, einschließlich Verwaltungsdaten, unter Einhaltung der Datenschutzvorschriften verarbeitet werden können.

Um die notwendigen Schlussfolgerungen zu ziehen und Empfehlungen auszuarbeiten, wurden im Rahmen der Studie folgende Aufgaben durchgeführt:

- eine Beschreibung des rechtlichen Rahmens auf EU-Ebene mit Auswirkungen auf die Monitoring- und Evaluierungsmaßnahmen des ESF+.

- ein Überblick über die nationalen Rechtsrahmen wurde gegeben, um weitere Einblicke zu gewinnen, wie eine Auswahl von neun Mitgliedstaaten (Österreich, Deutschland, Spanien, Frankreich, Irland, Italien, Polen, Rumänien und Schweden) den EU-Rechtsrahmen umsetzen und ergänzen.

- Bewertung von Beispielen für datensatz- und sektorspezifische Regelungen aus drei ausgewählten Mitgliedstaaten (Österreich, Spanien und Rumänien), um einen tieferen Einblick in die Vielfalt und Vielzahl der nationalen Rechtsvorschriften zu erhalten, die für Datensätze zu berücksichtigen sind, die im Besitz von staatlichen Behörden stehen.

- Analyse von Datenschutzaspekten, die für die Monitoring- und Evaluierungsmaßnahmen des ESF+ relevant sind, einschließlich der einschlägigen Rechtsgrundlagen, Vorschriften und nationalen Praktiken in Bezug auf die Wiederverwendung von Daten, die Einwilligung, besondere Kategorien personenbezogener Daten, die Übermittlung von Daten, die Datenverknüpfung, die Datenspeicherung und die Informationspflicht der betroffenen Personen.

- Entwicklung von Modellen für den Zugang zu Verwaltungsdaten in neun Mitgliedstaaten, einschließlich einer vertieften Prüfung von drei Mitgliedstaaten (Österreich, Spanien und Italien) und der entsprechenden rechtlichen Verpflichtungen und Bedingungen für den Zugang zu diesen Daten.

- Durchführung von 50 Interviews mit einem breiten Spektrum relevanter Stakeholder in neun Mitgliedstaaten, ergänzt durch mehrere Runden von Folgefragen, um Praktiken, Herausforderungen und mögliche Lösungen für die Verarbeitung von Daten zum Zweck der Umsetzung, des Monitoring und der Evaluierung von ESF/ESF+-Projekten zu ermitteln. Im Rahmen der Studie wurde auch eine Fokusgruppe mit Teilnehmern der wichtigsten Interessengruppen aus 13 Mitgliedstaaten organisiert, um die wichtigsten anstehenden Fragen zu erörtern und gemeinsam nach möglichen Lösungen zu suchen.

Die Ergebnisse der rechtlichen Untersuchungen und der Konsultationen mit den Stakeholdern wurden in erster Linie dazu genutzt, Herausforderungen im Zusammenhang mit der Verarbeitung von Verwaltungsdaten für die Monitoring- und Evaluierungsmaßnahmen des ESF/ESF+ zu identifizieren und Empfehlungen zur Bewältigung dieser Herausforderungen zu entwickeln. Diese Herausforderungen und Empfehlungen werden im letzten Abschnitt dieser Zusammenfassung sowie in Kapitel 7 dieses Berichts dargelegt. Es gibt jedoch eine Reihe von Schlussfolgerungen, die im Folgenden vorgestellt werden und die als Ergebnis der rechtlichen Untersuchungen und der Konsultationen hervorzuheben sind und die die angemessensten Rechtsgrundlagen und Modelle der Mitgliedstaaten für den Zugang zu Verwaltungsdaten betreffen.

Geeignete Rechtsgrundlagen für die Verarbeitung von Verwaltungsdaten

Aus den Rechtsquellen und der Rechtsprechung auf EU-Ebene geht hervor, dass zwar mehrere Rechtsgrundlagen in der Datenschutz-Grundverordnung[9] (weiter DSGVO) herangezogen werden können, um die Verarbeitung von (einschließlich des Zugriffs auf) Verwaltungsdaten von Teilnehmern und Nichtteilnehmern zu legitimieren, die geeignetsten Rechtsgrundlagen jedoch zu sein scheinen:

- die Erfüllung einer rechtlichen Verpflichtung[10] und
- die Erfüllung einer Aufgabe, die im öffentlichen Interesse[11] liegt.

Beide Rechtsgrundlagen lassen den Mitgliedstaaten einen gewissen Ermessensspielraum in dem Sinne, dass die nationalen Gesetze zur Umsetzung der DSGVO spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO enthalten können, wie in Artikel 6 Absatz 2 und 3 der DSGVO festgelegt.

In den neun Mitgliedstaaten, die für diese Studie befragt wurden, war die Einwilligung als Rechtsgrundlage bisher die gängigste Praxis bei der direkten Erhebung personenbezogener Daten von ESF-Teilnehmern. Die Verwendung der Einwilligung als Rechtsgrundlage kann jedoch mit einem hohen Verwaltungsaufwand verbunden sein, und die rechtliche Analyse in Abschnitt 5.3 dieser Studie zeigt, dass die Verwendung der Einwilligung als Rechtsgrundlage oft nicht geeignet ist, insbesondere dann nicht, wenn personenbezogene Daten von einer öffentlichen Behörde erhoben werden.

Eine weitere Herausforderung im Zusammenhang mit der Einwilligung besteht darin, dass die nationalen Behörden bei Problemen mit ihrer Validität nicht rückwirkend von der Einwilligung zu einer anderen Rechtsgrundlage übergehen können, um die Verarbeitung zu rechtfertigen. Nur in bestimmten Fällen kann die Einwilligung durch eine andere Rechtsgrundlage ersetzt werden, die der Situation besser entspricht, z. B. im Falle des

[9] Artikel 6 Datenschutz-Grundverordnung.

[10] Artikel 6 Abs. 1 lit. c) Datenschutz-Grundverordnung.

[11] Artikel 6 Abs. 1 lit. e) Datenschutz-Grundverordnung.

Widerrufs der Einwilligung oder der Verarbeitung für einen neuen/zusätzlichen Zweck. Jede Änderung muss jedoch den betroffenen Personen gemäß den Informationspflichten der Artikel 13 und 14 DSGVO mitgeteilt werden.

Darüber hinaus ist es besonders schwierig, sich auf eine ausdrückliche Einwilligung zu verlassen, um das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten aufzuheben. Stattdessen ist die Anwendung der Ausnahmen in Artikel 9 Abs. 2 lit. g) über die Verarbeitung aus wichtigem öffentlichen Interesse, Artikel 9 Abs. 2 lit. h) über die Verarbeitung aus medizinischen Gründen oder Artikel 9 Abs. 2 lit. i) über die Verarbeitung von Daten im öffentlichen Interesse im Bereich der öffentlichen Gesundheit besser geeignet.

Es gibt drei Möglichkeiten für die Weiterverwendung von Verwaltungsdaten, nämlich (i) wenn der Zweck der Weiterverwendung von Verwaltungsdaten mit dem ursprünglichen Zweck der Verarbeitung dieser Verwaltungsdaten vereinbar ist; (ii) wenn eine Rechtsgrundlage für die Weiterverwendung von Verwaltungsdaten im nationalen Recht besteht; oder (iii) wenn die Weiterverwendung zum Zweck der wissenschaftlichen Forschung erfolgt. In Bezug auf Letzteres gibt es zwar Interpretationen und Argumente sowohl für als auch gegen die Annahme, dass von den Verwaltungsbehörden durchgeführte oder in Auftrag gegebene Auswertungen als wissenschaftliche Forschung angesehen werden können, doch kann auf der Grundlage von Artikel 5 Abs. 1 lit. b) der DSGVO in Verbindung mit Artikel 89 Abs. 1 argumentiert werden, dass Auswertungen unter bestimmten Umständen als solche Forschung angesehen werden können.

Modelle für den Zugang zu Verwaltungsdaten in den Mitgliedstaaten

Auf der Grundlage von Interviews und Literaturrecherchen sind die meisten Ländermodelle für den Zugang zu und die Verknüpfung von Verwaltungsdaten für die Monitoring- und Evaluierungsmaßnahmen des ESF/ESF+ dezentral auf verschiedene Institutionen und Regierungsebenen verteilt. Schweden ist der einzige der neun in dieser Studie untersuchten Mitgliedstaaten, der sein Modell des Zugangs zu Verwaltungsdaten für die Monitoring- und Evaluierungsmaßnahmen des ESF/ESF+ zentralisiert hat. Das Modell des Zugangs zu Verwaltungsdaten in Schweden könnte als zentralisiert und harmonisiert bezeichnet werden, da die gesamte Datenverarbeitung und -verknüpfung beim schwedischen Statistikamt zentralisiert ist. Die Modelle für den Zugang zu Verwaltungsdaten in allen anderen acht Mitgliedstaaten (Österreich, Deutschland, Spanien, Frankreich, Irland, Italien, Polen und Rumänien) sind dezentralisiert. In diesen Mitgliedstaaten kann es zentrale Datenbanken geben, in denen Daten gespeichert werden, die direkt bei den ESF/ESF+-Teilnehmern erhoben werden, und die Verwaltungsstellen können eine koordinierende Rolle spielen. Vorhandene Verwaltungsdaten, die zur Ergänzung und Verknüpfung von Daten für das Monitoring und die Evaluierung verwendet werden, werden jedoch weder zentral koordiniert noch verarbeitet.

Gutachter können auch auf Verwaltungsdaten zugreifen, ohne die zuständige Verwaltungsstelle informieren zu müssen. In Spanien, Frankreich, Polen und Rumänien beispielsweise muss der Zugriff auf Verwaltungsdaten bei jeder einzelnen Einrichtung erfolgen, die diese Daten verwaltet, und die Verfahren hierfür können je nach Einrichtung und Region unterschiedlich sein. In Irland gibt es Versuche, die Datensätze zu harmonisieren, z. B. über den Jobseekers Longitudinal Dataset (JLD), und es gibt Beispiele für kohärente Modelle, die von einzelnen zwischengeschalteten Stellen mit Zugang zu ihren eigenen Verwaltungsdaten verwendet werden. Allerdings gibt es kein landesweites Modell, und die Verwaltungsstelle ist an diesem Prozess nicht beteiligt. Schließlich verwaltet die österreichische Verwaltungsstelle zwar eine zentrale Datenbank mit den für ESF/ESF+-Zwecke erhobenen Teilnehmerdaten, der Zugang zu den Verwaltungsdaten für ESF/ESF+-Zwecke ist jedoch weder zentralisiert noch harmonisiert.

Dezentrale Datenverarbeitungsmodelle können Herausforderungen mit sich bringen, wenn es um die Effektivität und Effizienz der Verarbeitung von Verwaltungsdaten für die Monitoring- und Evaluierungsmaßnahmen des ESF/ESF+ geht. Diese Herausforderungen gehören zu den anderen Problemfeldern, die in dieser Studie identifiziert wurden und die im nächsten Abschnitt zusammen mit den Empfehlungen zur Überwindung dieser Herausforderungen vorgestellt werden.

Die wichtigsten ermittelten Herausforderungen und Empfehlungen zu deren Bewältigung

Herausforderungen und Empfehlungen im Zusammenhang mit der Ermittlung und Wahl der am besten geeigneten Rechtsgrundlage

Eine in dieser Studie festgestellte Herausforderung besteht darin, dass es für die Verwaltungsstellen, die Begünstigten und die Gutachter problematisch sein kann, sich zwischen den möglichen Rechtsgrundlagen zurechtzufinden und zu beurteilen, welche die geeignetste, wirksamste und effizienteste für die Datenverarbeitung bei dem Monitoring und der Evaluierung des ESF+ ist. Daher empfiehlt die Studie Folgendes:

- Die Mitgliedstaaten und die Verwaltungsstellen von ESF+ sollten ihre nationale Datenschutzbehörde zu den geltenden Datenschutzvorschriften, einschließlich der Rechtsgrundlage für die Verarbeitung personenbezogener Daten zum Zweck der Evaluierung und des Monitorings von ESF+, konsultieren, wenn es Zweifel an den nach nationalem oder EURecht verfügbaren Möglichkeiten gibt. Wird eine Lücke in den Rechtsvorschriften festgestellt, sollten die Mitgliedstaaten mögliche Gesetzesinitiativen in Erwägung ziehen, um klare Datenschutzvorschriften, einschließlich einer Rechtsgrundlage für die Weiterverwendung von Verwaltungsdaten für die Zwecke der Monitoring- und Evaluierungsmaßnahmen von ESF+, zu schaffen.

Herausforderungen und Empfehlungen im Zusammenhang mit der Wiederverwendung von Verwaltungsdaten und/oder der weiteren Nutzung von Daten für die wissenschaftliche Forschung

Verwaltungsdaten in bestehenden nationalen Datenbanken können nur dann für Monitoring- und Evaluierungszwecke im Rahmen von ESF+ weiterverarbeitet werden, wenn die erforderlichen Bedingungen erfüllt sind (z. B. wenn die Weiterverwendung mit dem ursprünglichen Zweck vereinbar ist, einschließlich des Falls, dass die Verarbeitung für ESF+-Zwecke als wissenschaftliche Forschung angesehen werden könnte) oder wenn es eine spezifische Rechtsgrundlage für die Weiterverwendung gibt. Wie oben beschrieben, gibt es im Fall von Bewertungen sowohl Argumente dafür, dass von den Verwaltungsbehörden durchgeführte oder in Auftrag gegebene Bewertungen als wissenschaftliche Forschung angesehen werden können, als auch dafür, dass sie nicht als solche gelten können, auch abhängig von Umfang und Qualität der Methodik der betreffenden Evaluierungen. Daher empfiehlt die Studie Folgendes:

- Die Mitgliedstaaten sollten eine klare Rechtsgrundlage für die Weiterverwendung von Verwaltungsdaten auf nationaler Ebene schaffen.

- Die nationalen Datenschutzbehörden sollten Stellungnahmen/Leitlinien dazu ausarbeiten, wann die Wiederverwendung von Verwaltungsdaten als Verarbeitung zu "kompatiblen Zwecken" angesehen werden kann, wann die Weiterverarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken möglich ist,

wann die Evaluierung des ESF+ als "wissenschaftliche Forschung" angesehen werden kann und welche Schutzmaßnahmen für die betroffenen Personen angemessen sind.

- Die nationalen Verwaltungsbehörden sollten Vereinbarungen über die gemeinsame Nutzung von Daten abschließen, um den Austausch von Verwaltungsdaten für ESF+-Zwecke zu erleichtern.

Herausforderungen und Empfehlungen im Zusammenhang mit der Verarbeitung besonderer Kategorien von personenbezogenen Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten erfordert sowohl eine geeignete Rechtsgrundlage als auch eine Ausnahme, um das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten aufzuheben. Da die Verarbeitung besonderer Kategorien personenbezogener Daten einen stärkeren Eingriff in die Rechte der betroffenen Personen darstellt, verlangt die DSGVO, dass besondere Garantien zum Schutz der personenbezogenen Daten von Personen gesetzlich vorgesehen werden. Die Befragung der Stakeholder ergab, dass die Begünstigten in den meisten der in dieser Studie untersuchten Mitgliedstaaten für den ESF-Programmplanungszeitraum 2014-2020 besondere Kategorien von personenbezogenen Daten erhoben haben. In einigen Mitgliedstaaten war es jedoch nicht immer möglich, diese Daten zu verarbeiten, weshalb die Studie Folgendes empfiehlt:

- Bei der Verarbeitung besonderer Kategorien personenbezogener Daten sollte das Prinzip der Datenminimierung gelten, auch durch Anonymisierung.

- Die Mitgliedstaaten stellen sicher, dass es eine Rechtsgrundlage für die Verarbeitung sowie eine anwendbare Ausnahmeregelung zur Aufhebung des Verbots der Verarbeitung besonderer Kategorien personenbezogener Daten gibt und dass die nach nationalem Recht vorgeschriebenen angemessenen Garantien vorhanden sind.

- Die Verwaltungsbehörden lassen sich erforderlichenfalls von Datenschutzexperten (nationale Datenschutzbehörden, behördliche Datenschutzbeauftragte oder Berater) zu den geltenden Vorschriften und geeigneten Garantien beraten.

- Für die Verarbeitung besonderer Kategorien personenbezogener Daten werden alternative Methoden verwendet (z. B. fundierte Schätzungen der Begünstigten).

Herausforderungen und Empfehlungen im Zusammenhang mit dem mangelnden Verständnis und/oder Bewusstsein für den nationalen Rechtsrahmen für die Verarbeitung von Verwaltungsdaten

Um zu verstehen, wie personenbezogene Daten in den Mitgliedstaaten verarbeitet werden sollten, müssen mehrere Rechtsvorschriften berücksichtigt werden. Die EU-Charta und die Europäische Menschenrechtskonvention müssen beachtet werden, und jede Datenverarbeitung muss auch den Bestimmungen der DSGVO, Verordnung (EU) 2021/1060 (die Dachverordnung), und der ESF+-Verordnung entsprechen. Darüber hinaus müssen auch die nationalen Rechtsvorschriften beachtet werden, und auch hier sind mehrere Ebenen von Instrumenten zu berücksichtigen. Die Verarbeitung personenbezogener Daten muss den Anforderungen der nationalen Verfassungen, den nationalen Rechtsvorschriften zur Ergänzung der DSGVO, den nationalen (oder sogar

regionalen) sektoralen und datensatzspezifischen Rechtsvorschriften sowie dem sektorspezifischen Datenschutzrecht entsprechen.

Während in übergreifenden Rechtsinstrumenten wie der DSGVO allgemeine Regeln festgelegt sind, enthalten diese nicht immer detaillierte Vorschriften für den Umgang mit jeder spezifischen Art von Daten und erlauben es den Mitgliedstaaten daher oft, diese Regeln anzupassen oder spezifischere Regeln vorzusehen, die den Erfordernissen der Verarbeitungen in bestimmten Sektoren Rechnung tragen. Bestimmte Rechtsgrundlagen der DSGVO[12] lassen den Mitgliedstaaten den Spielraum, bestimmte Aspekte der Datenverarbeitung in ihren nationalen Rechtsvorschriften weiter zu regeln. In Ermangelung klarer Leitlinien kann es für die an dem Monitoring und Evaluierung des ESF+ beteiligten Akteure daher schwierig sein zu verstehen, welche Regeln gelten und welche Möglichkeiten sie mit sich bringen. Daher empfiehlt die Studie den Stakeholdern Folgendes:

- Erwägen Sie die Möglichkeiten, die die nationalen Rechtsvorschriften in Kombination mit dem EU-Recht bieten, um die Verarbeitung von Verwaltungsdaten im Rahmen von ESF+ zu erleichtern, und nicht deren Einschränkungen.

- Beratung, Anleitung und/oder Teilnahme an Schulungen für Datenschutzexperten (nationale Datenschutzbehörden, behördliche Datenschutzbeauftragte oder Berater) ermöglichen, gegebenenfalls zusammen mit anderen Datenschutzexperten, um den geltenden Rechtsrahmen und die Anforderungen, die für die Verarbeitung von Verwaltungsdaten zum Zweck der Monitoring- und Evaluierungsmaßnahmen des ESF+ gelten, besser zu verstehen.

- Gegebenenfalls Durchführung von Datenschutz-Folgenabschätzungen für neue Projekte und Förderung des Austauschs von vielversprechenden Beispielen oder Vorlagen für solche Abschätzungen.

Herausforderungen und Empfehlungen im Zusammenhang mit der geringen Interoperabilität der nationalen Register und dem Grad der Zentralisierung der Datenverarbeitung

Eine häufige Herausforderung beim Zugang zu Verwaltungsdaten besteht darin, dass die für die Monitoring- oder Evaluierungsmaßnahmen des ESF/ESF+ relevanten Daten bei verschiedenen Institutionen und/oder auf unterschiedlichen Verwaltungsebenen gespeichert sind. Diese Daten können in einigen Fällen schwer zu vergleichen sein, auch mit ESF+-Indikatoren, was teilweise auf unterschiedliche Definitionen der Daten zurückzuführen ist. So kann die dezentrale Bereitstellung von Daten zu Problemen bei der Interoperabilität nationaler Register führen, die für die Monitoring- oder Evaluierungsmaßnahmen des ESF+ relevant sind. Darüber hinaus können für verschiedene Datensätze unterschiedliche Datenschutzbestimmungen und unterschiedliche Einwilligungserfordernisse gelten. Daher empfiehlt die Studie Folgendes:

- Prüfung der Möglichkeit einer Zentralisierung der Datenverarbeitung, einschließlich des Hostings von Daten, die für die Monitoring- und Evaluierungsmaßnahmen des ESF+ relevant sind.

- Förderung der Zentralisierung der Verwaltung und Koordinierung des Zugangs zu Verwaltungsdaten für die Zwecke der Monitoring- und Evaluierungsmaßnahmen des ESF+.

[12] Artikel 6 Abs. 1 lit. c) und e) Datenschutz-Grundverordnung.

- Erwägen Sie den Einsatz der Pseudonymisierung als Technik zur Minderung von Datenschutzrisiken.

Herausforderungen und Empfehlungen in Bezug auf vermeidbare Kosten, Verzögerungen und Dateninkompatibilität

Der Zugang zu Verwaltungsdaten kann zeitaufwendig sein, und es kann eine lange Wartezeit geben, nachdem ein Antrag gestellt wurde. Der Zugang zu Verwaltungsdaten kann auch mit finanziellen Kosten verbunden sein, da Organisationen, insbesondere externe Gutachter, möglicherweise Daten von den Dateninhabern kaufen müssen. Darüber hinaus können die Daten von den Dateninhabern unterschiedlich definiert werden, und die Daten sind möglicherweise nicht zwischen den Datenbanken der Mitgliedstaaten vergleichbar. Daher empfiehlt die Studie:

- Im Voraus zu planen, welche Verwaltungsdaten benötigt werden, um die direkte Datenerhebung für das Monitoring und die Evaluierung im Rahmen von ESF+ zu ergänzen oder zu ersetzen.

- Die Verwaltungsstellen sollten die Planung mit den Inhabern von Verwaltungsdaten koordinieren, die möglicherweise wissen, welche Daten verfügbar sind.

Herausforderungen und Empfehlungen im Zusammenhang mit einem Mangel an gemeinsamen Lernen der Mitgliedstaaten in Bezug auf datenschutzbezogene Fragen des Zugangs zu Verwaltungsdaten für ESF/ESF+-Zwecke

Es gibt Praktiken, die angewendet werden können, um die Herausforderungen beim Zugang zu Verwaltungsdaten zu überwinden. Während der Interviews in dieser Studie wurden mehrere Beispiele für gute Praktiken beim Zugang zu Verwaltungsdaten für Monitoring- und Evaluierungszwecke im Rahmen von ESF+ ermittelt. Daher empfiehlt die Studie:

- Die Mitgliedstaaten und die Verwaltungsstellen sollen gute Praktiken für den Zugang zu Verwaltungsdaten für ESF/ESF+-Zwecke austauschen.

- Die zuständigen EU-Behörden sollen weiterhin Kontaktstellen einrichten, bei denen sich die einschlägigen Stakeholder aus den Mitgliedstaaten treffen und vernetzen können. Gegebenenfalls Einbeziehung der Datenschutzbehörden in solche Foren.

- Ausarbeitung eines praktischen Dokuments und/oder Handbuchs für die Mitgliedstaaten und/oder die zuständigen Behörden.

Abbreviations used

Abbreviation	Explanation
AEPD	Spanish Data Protection Authority (*Agenica Espanola Proteccion Datos*)
Af	Swedish Public Employment Service (*Arbetsförmedlingen*)
ANSPDCP	Romanian Data Protection Authority (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal)
APPD	Polish Act of 10 May 2018 on the Protection of Personal Data (*Ustawa z 10 maja 2018 o ochronie danych osobowych*)
BDSG	German Federal Data Protection Act (*Bundesdatenschutzgesetz*)
BfDI	German Data Protection Authority (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*)
CAD	Digital Administration Code
CIE(s)	Counterfactual Impact Evaluation(s)
CJEU	Court of Justice of the European Union
CNMC	National Competition Authority
CNIL	French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*)
CPR 2021	Common Provisions Regulation / Regulation (EU) 2021/1060
CPR 2013	Common Provisions Regulation / Regulation (EU) No 1303/2013
DG EMPL	European Commission's Directorate-General for Employment, Social Affairs and Inclusion
DPA(s)	Data Protection Authority(ies)
DPIA	Data protection impact assessment
DPO	Data Protection Officer

Abbreviation	Explanation
DSB	Austrian Data Protection Authority (*Datenschutzbeuftragter*)
DSG	Austrian Federal Act concerning the Protection of Personal Data (*Bundesgesetz über den Schutz personenbezogener Daten – Datenschutzgesetz*)
EaSI	Employment and Social Innovation programme
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EGF	European Globalisation Adjustment Fund
ENS	National Security Scheme
ERDF	European Regional Development Fund
ESI Funds	European Structural and Investment Funds
ESF	European Social Fund
ESF Regulation	Regulation (EU) No 1304/2013
ESF+	European Social Fund Plus
ESF+ Regulation	Regulation (EU) 2021/1057
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
GDPR	General Data Protection Regulation
IMY	Swedish Data Protection Authority (*Integritetsskydds myndigheten*)
ISTAT	Italian National Institute of Statistics

Abbreviation	Explanation
LIL	French Law on information technology, files and freedoms (*Loi relative à l'informatique, aux fichiers et aux libertés*)
LOPDGDD	Spanish Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights (*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*)
MEF IGRUE	Italian Ministry of Economy and Finance (MEF) General Inspectorate for Financial Relations with the European Union (IGRUE)
PUP	Poviat labour office
SCB	Statistics Sweden
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UAFSE	Administrative Unit for the European Social Fund
UODO	Polish Data Protection Authority (*Urząd Ochrony Danych Osobowych*)
WP29	Article 29 Working Party

1. Introduction

1.1. Brief policy background

Cohesion Policy represents one of the EU's main instruments for the achievement of EU2020 objectives and targets. In the 2014-2020 programming period, coordination and coherence between Cohesion Policy and the other EU policies contributing to regional development have been strengthened by laying down the Common Provisions Regulation (CPR 2013)[13] together with the Delegated Regulation (EU) No 480/2014[14]. The CPR 2013 provides strategic guiding principles and governing instruments for the European Structural and Investment (ESI) Funds and – for the European Social Fund (ESF) – is complemented by Regulation (EU) No 1304/2013 of the European Parliament and of the Council of 17 December 2013 (ESF Regulation)[15]. In terms of provisions for data collection, monitoring and evaluation, both regulations provide relevant information: the first providing the general principles, and the second presenting useful tools such as the list of the common indicators.

The European Social Fund Plus (ESF+) brings together four funds that were separate in the 2014-2020 programming period, namely: under shared management: the ESF, the Youth Employment Initiative and the Fund for European Aid to the most Deprived (scope of the proposed study); under direct and indirect management: the Employment and Social Innovation programme (EaSI). For the current period, the Cohesion Policy Regulations for the 2021-2027 programming period entered into force on 1 July 2021; among them, the Common Provisions Regulation (CPR 2021)[16] and the European Social Fund+ Regulation (ESF+ Regulation)[17].

The ESF+ aims at enhancing coherence and synergies between the various funds from the 2014-2020 programming period, increasing flexibility and streamlining and simplifying the programming and management of the funding and thereby reducing the administrative burden for the Member States. As such the overall architecture of the ESF+ monitoring and evaluation system still holds and will continue to provide the blueprint for understanding its functioning.

In the 2014-2020 programming period, important innovations in the programming, monitoring and evaluation of the ESF were introduced with a view to increasing the quality,

[13] European Commission. (2021). *Design and commissioning of counterfactual impact evaluations : a practical guidance for ESF managing authorities*. https://data.europa.eu/doi/10.2767/02762, Regulation (EU) No 1303/2013 of the European Parliament and of the Council of 17 December 2013 laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund and repealing Council Regulation (EC) No 1083/2006, OJ L 347, 20. 12. 2013, pp. 320-469. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013R1303

[14] Commission Delegated Regulation (EU) No 480/2014 of 3 March 2014 supplementing Regulation (EU) No 1303/2013 of the European Parliament and of the Council laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund, OJ L 138, 13.5.2014, p. 5–44. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0480

[15] Regulation (EU) No 1304/2013 of the European Parliament and of the Council of 17 December 2013 on the European Social Fund and repealing Council Regulation (EC) No 1081/2006, OJ L 347, 20. 12. 2013, pp. 470-486. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013R1304

[16] Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy (CPR).

[17] Regulation (EU) 2021/1057 of the European Parliament and of the Council of 24 June 2021 establishing the European Social Fund Plus (ESF+).

detail and robustness of monitoring data and impact evaluation of programmes. The 2021-2027 period aims at keeping continuity with the 2014-2020 period, whilst introducing some additional changes. Hence, while the overall architecture of the ESF is maintained in the ESF+, some adjustments are introduced to reduce the administrative burden of the Member States and the managing authorities.

Article 4 of the CPR 2021 provides that Member States may process personal data where necessary for their obligations under the CPR but must do so in accordance with the General Data Protection Regulation (GDPR)[18]. The ESF+ Regulation provides in Article 17(6) that Member States may enable their MAs and other ESF+ bodies to obtain data from administrative registers, in accordance with public interest processing legal bases found in Article 6(1)(c) (legal obligation) and Article 6(1)(e) GDPR (public interest). These legal bases provide, *inter alia,* that processing of personal data by public authorities will be lawful where Member State or EU law specifically enables such processing. Article 6(3) GDPR provides that such legal basis must determine the purpose of the processing or where processing is carried out on the basis of the public interest or official authority the processing must be necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

The study considers a selection of nine Member States and analyses the EU legislation and jurisprudence for the processing (reuse) of such administrative data for the purposes of monitoring and evaluation of ESF/ESF+ programmes, in accordance with GDPR, where Article 6(1)(c) or (e) is the applicable legal basis for processing data.

1.2. Scope and objectives of the study

The ESF+ is a publicly funded scheme; for accountability purposes and to ensure performance orientation, monitoring and evaluation are key elements. Without accurate, statistically robust data on (ESF/ESF+) participants (and entities), such monitoring and evaluation would be impossible. This implies a significant effort in collecting and validating quality data, particularly for managing authorities and beneficiaries who have (different) responsibilities for collecting them. With a view to improve the robustness and coherence of participants' data, while at the same time decreasing the burden for their collection, the European Commission encourages the Member States to use already existing administrative datasets that can provide or complement such data, as well as carry out robust evaluations, such as counterfactual impact evaluations (CIEs). Importantly, since much of this data must often be collected in personally identifiable form (whether from participants themselves or from administrative datasets), its use for monitoring and evaluation must comply with data protection rules at EU and Member State level.

The ESF/ESF+ is designed and implemented in partnership between the European Commission and national and regional authorities of the Member States. The GDPR provides a general legal framework for the protection of personal data leaving it to the discretion of Member States to further specify some of its rules. As a fundamental right enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (EU Charter)[19], the exercise of the right to the protection of personal data may be limited, but only if such limitation is proportionate, necessary, and genuinely meets objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The flexibility of legal instruments such as the GDPR are designed specifically to enable

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[19] Charter of Fundamental Rights of the European Union, (2012).

programmes such as the ESF/ESF+ to be implemented properly while ensuring individuals' right to the protection of their personal data.

This study shows ways in which it is possible to meet the monitoring and evaluation needs of ESF/ESF+ while ensuring the respect for the fundamental right to data protection. This study also proposes practical implementation tools based on a limited sample of country cases[20].

The study is designed to examine EU legislation and jurisprudence affecting the use of data[21] for the purposes of ESF/ESF+ monitoring and evaluation, to identify practical challenges in relation to reusing administrative data in line with the national data protection legal framework in nine Member States: Austria, Germany, Spain, France, Ireland, Italy, Poland, Romania, and Sweden. The choice of Member States is based on the allocation of funds for ESF+ in the coming period (2021-2027) and provides a diverse geographical, political and economic group for analysis, so that findings may be useful in relation to other Member States after completion of the study. Member States with centralised and regional/federal political and diverse legal systems are represented. Finally, whilst the selection of Member States takes into account the diversity, it also includes several Member States more likely to demonstrate good practices and to have extensive experience in database management and statistical monitoring and management of projects. Furthermore, the selection represents Member States with diverging views on how to reuse administrative data in line with the GDPR rules.

The study also examines practical aspects of ESF/ESF+ monitoring and evaluation, to identify other sources of difficulty or challenge for those involved in carrying out these functions in the nine Member States studied. While the legal analysis under Task 1 covers all nine Member States, the legal analysis for Task 2, which includes national data protection legislation, jurisprudence and decisions of national Data Protection Authorities (DPAs), focuses upon three Member States (i.e. Austria, Spain, and Romania). These three states are representative of the broader EU group, with a decentralised state (Spain) included, so that an in-depth analysis provides examples and findings that could support broader recommendations for the entire EU for ESF+ monitoring and evaluation. Moreover, the selection of three Member States for an in-depth analysis under Tasks 3.1 and 3.2 have been selected to represent different levels of centralised data processing systems: Austria, Italy, and Spain. Table 1 shows the selection of Member States covered in each of the four tasks carried out for this study.

Table 1: Selection of Member States for each task

Task (chapter)	Number of MSs	List of MSs for Study
Task 1 (chapter 4) (outline description of legal framework)	9	Austria, Germany, Spain, France, Ireland, Italy, Poland, Romania and Sweden With 3 examples of dataset and sectoral-specific legislation, from Austria, Romania, and Spain (one type of data from each MS)
Task 2 (chapter 5)	3	Austria, Spain, and Romania

[20] Please note that the study will not analyse all the Member State requirements for re-using administrative data in every case. As such, the study analyses the legal framework in each Member State and provides recommendations on how to implement general data protection principles.

[21] The term "data" primarily refers to "personal data" within the study. However, the broader term has been used to ensure that anonymised data, aggregated data or personal data otherwise rendered non-identifiable is included in the analysis.

Task (chapter)	Number of MSs	List of MSs for Study
Analysis of legal requirements		
Task 2.1 (chapter 5) legal basis	3	
Task 2.2 (chapter 5) transmission of data	3	
Task 2.3 (chapter 5) linking	3	
Task 2.4 (chapter 5) storage	3	
Task 2.5 (chapter 5) consent	3	
Task 2.6 (chapter 5) transparency	3	
Task 2.7 (chapter 5) special categories of personal data	3	
Task 3 (chapter 6) conditions to access data and models of data access	9	Austria, Germany, Spain, France, Ireland, Italy, Poland, Romania, and Sweden
Task 3.1 (chapter 6) Legal obligations and conditions to access data)	3	Austria, Spain and Italy
Task 3.2 (chapter 6) Models in accessing administrative data)	3	Austria, Spain and Italy
Task 3.3 (chapter 7) Good practices and issues	9	Austria, Germany, Spain, France, Ireland, Italy, Poland, Romania and Sweden
Task 4 (chapter 6) Recommendations and conclusions	9	Austria, Germany, Spain, France, Ireland, Italy, Poland, Romania and Sweden

1.3. Key challenges and solutions for the study

A key challenge for the study lay in the fact that the different sources of qualitative research do not refer to the same programming period, making triangulation of data a challenging exercise. Logically, the legal analysis is based on the currently applicable and valid EU and national legal framework (e.g., CPR 2021, ESF+ Regulation), whereas the information on the practices of the Member States obtained through stakeholder interviews refers mostly to the old ESF programming period (2014-2020). As the new programming period started in 2021, national stakeholders were only able to report on practical experiences with monitoring and evaluation of ESF programmes. In order to overcome this challenge, any information referring to practices under the ESF+ is clearly indicated. To this end, the report clearly indicates whether information relates to ESF or to ESF+ or if information applies to

both programming periods (ESF/ESF+). When triangulating data from legal analysis and stakeholder interviews, this report remains speculative as to how the new legislative framework might impact the national practices.

One challenge regarding the stakeholder interviews concerned the response rate, especially among the Data Protection Authorities (DPAs) and the National Statistical Institutes. To increase the response rate, the Country Experts scaled up the number of interview requests and sent reminders via e-mail and telephone calls. Also, regional statistical institutes were interviewed and DPAs were asked to share relevant opinions and guidelines issued regarding ESF/ESF+ monitoring and evaluation. Moreover, questions regarding the role of DPAs were asked to other stakeholder categories.

Another challenge regarding the stakeholder interviews concerned the understandability and answerability of the interview questions. To increase the understandability and answerability of the interview questions, follow-up questions were asked, and explanations were formulated during the interviews or via e-mail to capture the intentions of the general interview questionnaire.

A final challenge regarding the interviews, which also relates to the analysis of the interview answers, concerned the level of understanding of the key concepts used in the interview questions among the stakeholders. For example, regarding the difference between processing data for monitoring and evaluation purposes, and the difference between administrative data and data collected directly from ESF/ESF+ participants. One main solution to this challenge was to ask the interviewees to describe what data they use or collect in general. The data could then be categorised in the analysis phase.

Regarding the literature review and legal analysis, one of the main challenges encountered during desk research was the lack of specific literature, guidelines and case-law. Very few sources of information touch upon data protection issues in connection with ESF/ESF+ monitoring and evaluation. There are also only a few clear sources of information regarding legal instruments that regulate access to administrative data. To overcome these challenges, the data collection and analysis team needed to draw conclusions by researching and analysing general guidance and case law on processing administrative data by public authorities.

1.4. Purpose and structure of the Report

In accordance with the Technical Specifications and in light of the feedback received from the Commission, this report covers the following elements:

- Brief policy background, a description of the scope and objectives of the study and a description of the challenges encountered, and solutions found (Section 1);
- Overview of the methodological approach used in the study and information on whether any changes are required to the initially planned methodology (Section 2);
- Summaries and main conclusions from the interviews (Section 3);
- Results for Task 1 on the description of the legal framework in the EU and in all nine EU Member States (Section 4);
- Results for Tasks 2 (Tasks 2.1 - 2.7) regarding the analysis of the data protection aspects relevant to the monitoring and evaluation of ESF+ at EU and at Member State level covering three EU Member States (Section 5);

- Results from Task 3, excluding 3.3, on conditions to access data and models of data access (Section 6);

- Results from Task 3.3 on challenges and good practices, and results from Task 4 including conclusions and recommendations taking into account the results of the Focus Group (Section 7);

- Annexes with additional information from the work carried out to date, including the list of the literature reviewed (Annex I – References), the list of stakeholders interviewed (Annex II – List of interviews and additional consultations carried out), the summaries of interviews per Member State (Annex III – Interview country summaries), the results from the Focus Group meeting (Annex IV – Focus Group summary), and the list of national ESF/ESF+ and GDPR-implementing legislation (Annex V – ESF/ESF+ and data protection legislations).

2. Methodological approach

The methodological approach is based on the tasks outlined in the Technical Specifications and the approach presented in the Inception Report. The progress made to date; problems encountered, as well as any changes to the methodology are summarised below.

2.1. Overview of methodological approach

This study serves several purposes – it reports on legal requirements in EU and national laws in nine EU Member States regarding the use of data for ESF/ESF+ monitoring and evaluation, but also gathers stakeholder input to analyse the challenges experienced in reusing administrative data in line with the current rules. As a final step, the study proposes recommendations to address the potential shortcomings identified with a view to accessing administrative data. Four tasks are proposed in the Technical Specifications to carry out this work; our methodology expands upon these tasks, incorporating them into a set of project phases that covers all the activities needed to deliver the required results.

Our approach is based on our understanding of complex evaluations of policy and legal issues, requiring the collection and synthesis of information and perspectives from diverse sources and the development of sound, evidence-based conclusions that can provide input to the possible development of rules at EU level, where necessary, and of recommendations that may be implemented across all EU Member States.

The phases of the study were the following:

- Phase one: preliminary desk research, including a scoping questionnaire that was sent to members of the ESF+ Monitoring and Evaluation Partnership and/or of the ESF+ Data Network in each of the nine Member States analysed in this study. The phase was finalised with an Inception Report approved by the European Commission, containing an updated methodological approach and data collection methods.

- Phase two consisted of desk research for Tasks 1 and 2, and stakeholder interviews with a total of 50 stakeholders from the nine Member States analysed in this study. The phase was finalised with an Interim Report approved by the European Commission.

- In phase three, initial research was done for Task 3, and further research done for Task 4. In addition, draft challenges and recommendations were formulated, tested and discussed in a Focus Group meeting that gathered 16 stakeholders in 13 EU Member States.

- In phase four, all final research for Tasks 3 and 4 was conducted, and the conclusions and recommendations developed taking into account the results from the Focus Group.

Three detailed methodology chapters are presented below:

- Literature review and analysis;

- Interviews; and

- Focus group

2.2. Literature review and analysis

2.2.1. Identification of information gaps

Preliminary desk research entailed the identification and compilation of sources of information and available literature aiming at the identification of information gaps, which were later completed based on the Commission's suggestions, the scoping questionnaires as well as further data collection methods during the data collection and legal analysis phase.

The preliminary research carried out by the Data Collection & Analysis Team, under the guidance of the Project Management Team, covered a wide range of EU and national level sources regarding data collection and usage for statistical, monitoring, and public interest purposes. The reviewed information included legal and policy documents, studies and research reports, as well as academic literature. The overview of the sources reviewed is contained in Annex I (Section 8.1) below.

The first results of this literature review at EU and Member State level fed into the preparation of the methodological tools (for example, the scoping questionnaire, the interview template), in the selection of stakeholder participants and, ultimately, in the analysis itself.

2.2.2. EU level desk research and analysis

The second phase – data collection – consisted of an extensive collection of data at EU level, which included review of legal sources, literature, reports of the competent authorities and case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

Legal sources reviewed both under Tasks 1 and 2 included existing **EU legal framework for data protection** as it relates to ESF+ monitoring and evaluation, comprising a description of the relevant aspects of the GDPR, the EU Institutions Data Protection

Regulation[22] (where relevant), the EU Charter, and the European Convention of Human Rights, as well as the legislation governing ESF+ monitoring and evaluations, such as the Common Provisions Regulation (EU) 2021/1060 (CPR 2021) and Regulation (EU) 2021/1057 (ESF+ Regulation).

Additionally, the Data Collection & Analysis Team reviewed **case law** of the two European courts (the CJEU and the ECtHR), which provides interpretation of the legal provisions concerning the (re)use of data for ESF+ monitoring and evaluation. The case law review focused on cases commenting on the (re)use of participants and administrative data, and the jurisprudence surrounding the legal bases for processing under GDPR and applicable safeguards.

Important sources of information and guidance for researchers during the data collection and analysis phase were **opinions and guidelines from the EU data protection authorities**, namely, the European Data Protection Board (EDPB), its predecessor the Article 29 Working Party (WP29), as well as from the European Data Protection Supervisor (EDPS). These bodies are key sources when it comes to understanding data protection issues, thus the analysis of their publications was a key activity in our methodology.

Results of the EU level research feed into the analysis of Tasks 1 and 2 which is presented in this Final Report.

2.2.3. National level desk research and analysis

In parallel with the EU-level research, the data collection phase also included national level desk research in order to substantiate the analysis in Tasks 1 and 2.

National level legal research underpinning analysis in Task 1 comprises a description of the **domestic legal framework for data protection** as relevant to ESF+ monitoring and evaluation in the **nine Member States** selected for this study – Austria, France, Germany, Ireland, Italy, Poland, Romania, Spain and Sweden. The desk research in each Member State included legal mapping of national rules relating to collection, analysis, transmission and reuse of ESF+ monitoring and evaluation data, focusing on GDPR-implementing laws, CPR 2021 and ESF+ implementing legislation, Partnership Agreements and other legal sources (such as guidelines on programmes) as well as a brief description of the role of national Data Protection Authority (DPA) and courts with jurisdiction over data protection cases.

By way of several illustrative examples looking at the domestic sectoral and dataset-specific legislation that impacts the reuse of administrative data for ESF+ monitoring and evaluation, the national desk research aims to emphasise the sheer volume and the complexity of national rules when it comes to the processing of administrative data for ESF+ purposes.

A more **in-depth desk review** was performed in **three Member States** – Austria, Romania and Spain – in order to support the analysis of certain data protection aspects relevant to the evaluation and monitoring of the ESF+ in Task 2 of this study. The legal research conducted for these three Member States focused upon the national data protection legal framework, in particular national GDPR-implementation laws and any provisions in national CPR 2021 and ESF+ implementing legislation relevant to the aspects considered. In addition, national desk research aimed to gather examples of national DPAs decisions, opinions and guidelines of relevance to the aspects considered. Where Member States have both national (or federal) DPA and regional DPAs (such as in Spain), only the

[22] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

decisions of the former have been analysed. Finally, research also included examples of national jurisprudence, as applicable to each of the sub-tasks in Task 2.

The **legal analysis** at national level was conducted on the assumption that each Member State's implementing laws are in accordance with GDPR and do not represent any form of infraction from its requirements. Moreover, the national-level analysis was based upon national researchers' preliminary assessment of legislation, followed by detailed examination in translation by the Data Collection & Analysis Team. It is therefore possible that particular points of note or interest may be a result of incorrect translation of the text. Every effort has been made to ensure that translated texts and concepts are accurate.

Moreover, the focus of the national-level research was on the national data protection legal framework and **did not seek to provide an analysis of the sectoral or database-specific legislation** that applies to each potential ESF+ dataset in those Member States. Consequently, the analysis focuses on the data protection legal framework applicable to the processing of data by the public sector, as relevant to each aspect (sub-task).

Finally, in line with the requirements in the Technical Specifications[23] the analysis in Task 2 focuses on providing **illustrative examples** from three different Member States and does not aim to exclusively answer each of the research questions from a viewpoint of a specific national legal system. National examples provided throughout the analyses are likely to be illustrative of broader practices throughout the EU.

The data collection activities at national level were carried out by the **team of National Experts** under the guidance of the Data Collection & Analysis Team.

2.3. Interviews

The interviews give the opportunity to gather views and opinions of stakeholders on the challenges and possible solutions in the processing of data for the purpose of implementing, monitoring, and evaluating ESF/ESF+ projects in the nine Member States selected for the study. They ensure that ongoing parallel legal research remains focused on practical issues. The interviews were semi-structured, which comes with the advantage that they provide reliable and comparable qualitative data, but they also leave some room for specific points that we may have not been foreseen, but that the stakeholders might want to make.

We conducted 50 stakeholder interviews with representation from each of the nine Member States and each of the stakeholder types that were selected. The list of stakeholders and stakeholder types interviewed per Member State is given in Annex II of this report. Our Core Team, in particular the Deputy Project Manager, managed the stakeholder engagement with the support of the National Researchers.

The interviews aimed to: 1) provide information on the practical realities of implementing, monitoring and evaluating ESF/ESF+ programmes in Member States; 2) provide information on the restrictions and challenges encountered by ESF/ESF+ managing authorities in obtaining reliable data on project participants; and 3) identify issues and solutions experienced in relation to obtaining access to administrative data for monitoring and evaluation of ESF/ESF+ programmes in Member States. The interviews also enable the identification of issues of relevance to data protection law that may not have been foreseen by initial desk research.

[23] Technical Specifications, p. 10.

The Core Team prepared a semi-structured interview questionnaire modified per stakeholder type to guide the National Experts. The questionnaire included questions in different modules, with each module targeting specific types of stakeholders. The semi-structured nature of the interview allowed the National Experts to ask additional questions that are tailored to the particular situation and rules of their country. If interviewees were not able to answer particular questions, the interviewees were asked to develop relevant answers in more general terms.

The interviews were conducted by the national experts in the national language, to facilitate participation. Interviewees received the interview template ahead of the interview so that they were aware of the topics to be discussed and prepare accordingly. Each interview lasted approximately 30 to 60 minutes and were conducted online. Some of the interviewees preferred to answer the questions in written form.

The interviewers took notes during the interviews, summarised, and translated the answers into English. These summaries have been coded and summarised into country-level summaries which are available in Annex III.

The interview template comprised six question modules. The modules included questions relevant to different types of stakeholders, both to ensure that only relevant questions are asked during the interview and that questions elicit detailed responses from interviewees. When individual stakeholders were identified, their individual roles in the ESF/ESF+ monitoring and evaluation process were analysed. National Experts carrying out the interviews then selected the question modules most appropriate to that stakeholder.

2.4. Focus group

The Focus Group was held online on 16 March 2023, and lasted for 2.5 hours. 28 participants attended from 13 EU Member States, representing 16 organisations, of which 14 were ESF managing authorities. Also present, were one ESF evaluator, and one intermediary body.

To ensure the formulation of robust and practical solutions that combine the monitoring and evaluation needs of the ESF/ESF+ with the fundamental right to data protection, the aim of the focus group was to assess the main issues at stake and to jointly explore possible solutions. The discussion held supported the development of the final recommendations proposed in the study.

To support the discussion, a background paper was circulated to the invited participants prior to the meeting, explaining the purpose of the study and the focus group, the focus group methodology, and a number of issues and solutions that had been identified so far in the study.

The issues and solutions discussed were based on the results of desk research and interviews with key stakeholders in nine EU Member States (i.e., Austria, Germany, Spain, France, Ireland, Italy, Poland, Romania, and Sweden), combined with a more in-depth legal analysis of Austria, Spain, Romania, and Italy. Participants were invited to:

- provide feedback on the proposed issues at stake; and
- discuss possible solutions according to a set of criteria, i.e., relevance, political feasibility, legal feasibility, and administrative feasibility, which refer to the following definitions:

- **Relevance** refers to the extent to which the proposed solution addresses the problems faced by the different stakeholders.

- **Political feasibility** refers to the likelihood that the proposed solution will be accepted and implemented by the relevant decision-makers. Factors that can affect political feasibility include the current political climate, the level of support from key stakeholders, and the potential impact on existing policies or programmes.

- **Legal feasibility** refers to the compatibility of the proposed solution with existing laws and regulations. Factors that can affect legal feasibility include the need for new legislation or regulations, potential conflicts with existing laws or policies, and the potential for legal challenges.

- **Administrative feasibility** refers to the ability to implement the solution within the available administrative structures and procedures. Factors that can affect administrative feasibility include the capacity of the relevant government agencies or organisations to implement the solution, the need for new administrative processes or systems, and the potential for bureaucratic or administrative barriers.

The proposed solutions were grouped into three main themes:

- Understanding and complying with data protection law
- Overcoming national particularities
- Organisational issues affecting effective access to administrative data.

Under each theme, the focus group organisers described a number of challenges (issues) and solutions that respond to these challenges.

To facilitate the discussion, participants could first vote on the relevance of each sub-solution and then discuss the feasibility of implementing the relevant solutions. Participants could also suggest new solutions and develop why certain solutions are relevant or not, and why certain solutions are feasible or not.

Following the feedback and discussion during the focus group, the report team reconvened to consider the inputs in relation to the proposed recommendations. This ensured that all perspectives were taken into account when the team assessed and analysed the potential recommendations and fine-tuning each potential recommendation in light of the feedback received.

A summary of the Focus Group meeting is available in Annex IV.

3. Main conclusions from the stakeholder interviews

The following summary is a brief comparison based on the country summaries that are included in Annex III. The country summaries in the Annex summarise more deeply the data processing practices of each country, based on the interviews performed.

Note that the terms used in this section are defined as follows:

- Managing authority: the government department that is responsible for implementation of the Operational Programme.

- Intermediary body: any public or private body which acts under the responsibility of a managing or certifying authority, or which carries out duties on behalf of such an authority, in relation to beneficiaries implementing operations.

- Beneficiary: an organisation or individual to which a grant is awarded to implement an operation (project or programme).

- Participant: an individual person (or occasionally an organisation such as a small business) who takes part in projects funded by ESF, for their benefit. This could include receiving education, training, or even food and supplies.Participants' personal data: personal information that is collected from an individual person (or occasionally an organisation such as a small business) who takes part in projects funded by ESF/ESF+.

- Administrative data: data collected by a public authority for a particular purpose, for example tax records collected by the tax authority, and held in databases for that purpose. This 'pre-existing' data is called 'administrative data' in ESF and ESF+ monitoring and evaluation.

Note also that data processing practices described concerns mainly the practices during ESF's 2014-2020 programming period and after implementation of GDPR. During the period of the interviews, there were insufficient experiences regarding the current ESF+ programming period 2021-2027. If stakeholder responses refer to the new ESF+ programming period, this is clearly indicated.

3.1. Processing of ESF participants' personal data

3.1.1. Collecting and gaining consent for collecting ESF participants' personal data from participants

Beneficiaries' collection of personal data from participants

As indicated in Table 2, interviewees from all nine Member States stated that beneficiaries collect personal data directly from participants. According to interviewees from Austria, France, Ireland, Poland, and Sweden, these data include special categories of personal data. In Austria, France, Germany, Ireland, and Italy, interviewees state that beneficiaries also collect personal data regarding participants from public authorities. In Austria and Germany, such public authority refers to a database that is managed by the managing authority, and in France and Ireland intermediary bodies. In Italy, it refers to employment or jobseeker datasets/register. Moreover, interviewees in Germany and Sweden stated that in some cases, beneficiaries collect personal data regarding participants from other organisations. In Germany, such organisations refer to job centres and schools, and in Sweden the employers of the participants.

Table 2: Beneficiaries' collection of personal data regarding participants per Member State

Beneficiaries' collection of personal data regarding participants per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	Directly from participants, including special categories of personal data. Also, via the ZWIMOS database (a database that is managed by the ESF managing authority), including special categories of personal data. Participants give consent for their data to be transmitted.
France	Directly from participants, including special categories of personal data. Also, data from Pole Emploi (which is an ESF intermediary body), to verify the participants' employment status. These data are collected for both monitoring and evaluation purposes.
Germany	Directly from participants, including special categories of personal data. Also, from organisations such as job centres and schools and according to one interviewee from a regional managing authority.
Ireland	Directly from participants, including special categories of personal data. Also, in some cases, contact details and national registration numbers from the Department of Social Protection (which is an ESF intermediary body).
Italy	Directly from participants. One beneficiary also stated that it collects employment data from a regional database that can be accessible to operators in charge of professional education. .
Poland	Directly from participants, including special categories of personal data in certain cases.
Romania	Directly from participants
Spain	Directly from participants
Sweden	Directly from participants, including special categories of personal data, and in some cases from their employers.

Managing authorities' collection of personal data regarding participants

As indicated in Table 3, interviewees from several Member States stated that beneficiaries transmit personal data regarding participants to managing authorities, either directly or via intermediaries such as ESF intermediary bodies or central databases, although some managing authorities may access these data only anonymised and or aggregated. In Austria, France, Italy, and Poland, interviewees stated that managing authorities may access personal data regarding participants via regional and or central databases that store data that are transmitted by beneficiaries and or other public authorities. In Germany, Ireland, Spain, and Sweden, the managing authorities may access only anonymised or aggregated data. In Ireland and Spain, the data are instead processed by intermediary bodies, and in Sweden by Statistics Sweden. However, according to one beneficiary in Sweden, the managing authority has the right to access (only view and not store) participants' personal data but only samples for monitoring purposes. Moreover, managing authorities may collect personal data via surveys directly from participants which is the case in France and Spain according to interviewees. In Ireland, only the intermediary bodies and not the managing authority may collect personal data directly from participants.

Table 3: Managing authorities' collection of personal data regarding participants per Member State

Managing authorities' collection of personal data regarding participants. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	From a nation database called ZWIMOS.
France	The central managing authority has direct access to the central MaDémarcheFse database. It also collects data directly from participants.
Germany	Two regional managing authorities and the federal managing authority stated that they process only aggregated data.
Ireland	Only anonymised data via beneficiaries. Only intermediary bodies can collect data directly from participants via surveys, and use own data held by the intermediary body for monitoring and evaluation.
Italy	In the Marche region, monitoring data on ESF indicators are collected via a database called COMarche. For evaluation purposes, a database called ASIA. ANPAL, the National Agency for Active Employment Policies also collects data for monitoring and evaluation purposes through a central data base.
Poland	Regionally, through a database called SL, and nationally, a database called Syrius, which contains personal data regarding ESF participants. The two systems are integrated to enable tracking of participants. The managing authority is required to collect personal data from ESF participants necessary for monitoring and evaluation purposes.
Romania	n/a
Spain	For the national managing authority, the steps to obtain data for the purpose of monitoring or evaluation reports are usually surveys, interviews, and consultations during open processes in which the parties involved in the management of the Funds can intervene. The managing authority described that data collection is decentralised through intermediary bodies. The managing authority receives only aggregated data from the intermediary bodies.
Sweden	Anonymised data from Statistics Sweden. According to one beneficiary, the managing authority has the right to access (only view and not store) participants' personal data but only samples for monitoring purposes.

In summary - collection of personal data from participants and consent practices

As indicated above, there are examples of participants' personal data that are collected directly by the beneficiaries from the participants in all countries that are included in this study. There are also examples where project implementers managing authorities, intermediary bodies, and evaluators collect personal data directly from participants. The types of data vary depending on the programme, project, and the ESF indicators that follow and include special categories of personal data. Interviewees from Germany and Spain mentioned that there are certain limiting restrictions on collecting this type of data.

Table 4 shows an overview of the collection of personal data directly from participants and consent practices per Member State assessed in this study. The process of collecting personal data from participants is relatively similar from country to country. Normally, beneficiaries and/or evaluators collect data via surveys that are sent directly to participants together with a consent form that the participants need to sign. In Spain, additional special consent forms are needed for special categories of personal data. Surveys may be sent several times before and after projects depending on the reporting and evaluation requirements. In Sweden, an external evaluator mentioned that it also gathers additional information via surveys and interviews. To get in contact with participants, the evaluator either receives contact details from the managing authority or sends it through to beneficiaries that can forward the survey to relevant project participants.

From the interview answers, only in Sweden was there an explicit example of a stakeholder that for their ESF projects do not systematically collect consent to collect, share, and use personal information about project participants. The Swedish Public Employment Service (Af), which is both an administrative data holder and a beneficiary that manages most ESF projects in Sweden, does not use explicit consent as a legal basis for collecting and sharing information about ESF participants. Instead, they use, according to Af's own interpretation, as a legal basis their legal obligation to carry out ESF projects, in accordance with Article 6(1)(c) of the GDPR[24] which enables processing when it is necessary for compliance with a legal obligation to which the controller is subject, along with a number of other legislative acts[25]. Their previous experience with using explicit consent to collect data was that it comes with a heavy administrative burden. Moreover, explicit consent in this context would, according to Af, not fulfil the requirement of freely given consent under the GDPR because many of the participants are dependent on Af through other contexts for receiving unemployment benefits, and many training sessions are not voluntary for unemployed participants as they are a condition for the continuation of unemployment benefits.

Table 4: Collection of personal data directly from participants and consent practices per Member State

Collection of personal data directly from participants and consent practices per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	Beneficiaries can collect personal data, including special categories of personal data. Some personal data that the beneficiaries are required to collect are necessary for the participants to be eligible for ESF funding. According to one beneficiary, participants are informed about the use of the data and sign a consent form.
France	Beneficiaries can collect personal data, including special categories of personal data. 'Participants' personal data are collected in several steps before and after implementation of ESF projects according to one interviewee.
Germany	Beneficiaries collect personal data from ESF participants before and after implementation of projects. The type of data collected depends on the project. Data on all common and programme-specific indicators are collected, including special categories of personal data.

[24] Article 6(1)(c), GDPR.

[25] (1) TVFS 2016:1 – provisions on ESF 2014-2020 from the Swedish Agency for Economic and Regional Growth, on obligations to share information. . (2) Ordinance (2015:62), Section 9. – on state support regarding ESF. It says that a beneficiary is obliged to share information with the Swedish ESF-council to evaluate the ESF, to fulfil Sweden's responsibilities to the European Commission according to Regulation (EU) 651/2014 and Regulation (EU) 1407/2013. (3) The following Swedish laws: Law (2018:259) and Law (2002:546) Section 5: 2 regarding data sharing in accordance with law or ordinance. (4) The following Swedish law: The Privacy Law (2009:400), 10 kap. Sections 2 and 28 (that stipulate that data sharing can occur for the public authority to fulfil its obligations and if they have a legal obligation to do so).

Collection of personal data directly from participants and consent practices per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Ireland	According to beneficiaries and intermediary bodies, ESF participants' personal data, including special categories of personal data can be collected. The data subjects need to give explicit consent to data processing. Types of personal data depend on the project. Data are normally collected via surveys before and after projects.
Italy	One beneficiary mentioned that they collect information that does not belong to special categories of personal data. The information is collected via a standard registration form for the region, including a consent form.
Poland	Depending on the programme, special categories of data can be collected on a voluntary basis.
Romania	If personal data are collected directly from participants, a consent form is used. The type of data collected depends on the context, but no examples were mentioned regarding special categories of data.
Spain	The steps to obtain participants' personal data for the purpose of monitoring or evaluation reports are usually surveys, interviews, and other consultations. In no case, neither special categories of data nor microdata of individual persons are handled due to data protection law. To handle special categories of personal data, consent is required from everyone.
Sweden	Personal data, including special categories of data, can be collected directly from participants by both beneficiaries and evaluators according to interviewees. Beneficiaries usually collect consent from participants for processing their data. However, the most dominant beneficiary, the Public Employment Service, uses another legal basis, based on their legal obligation to carry out ESF projects.

3.1.2. Storing ESF participants' personal data

Table 5 shows an overview of how ESF participants' personal data are stored in the nine Member States included in this study, according to interviewees. The nine countries (excluding Romania as there are no sufficient answers regarding storing participants' personal data) can be divided between having centralised, semi-decentralised, and decentralised data storing systems regarding participants' personal data that are collected for monitoring and or evaluating the ESF.

While collection and consent systems seem to be relatively similar among the countries included in this study, their data storing practices seem to differ to a greater extent. Also, in some countries, there are differences between regions and levels of government. Austria, France, Poland, and Sweden have a central system to store participants' data. However, data may be stored at different levels and by different actors before it is gathered or aggregated to a national central database. For example, in Austria, the managing authority is obliged by law to store data in a special ESF/ESF+ database called ZWIMOS (in 2014-2020) and IDEA (in 2021-2027), where beneficiaries report data for both monitoring and evaluation purposes. Similarly, in Sweden, Statistics Sweden is a central institution for processing personal data about ESF participants.

Italy has a system that can be placed in the middle between the centralised and decentralised systems. The Ministry of Economy and Finance (MEF) General Inspectorate for Financial Relations with the European Union (IGRUE) manages a national monitoring system. However, the system manages information on physical, financial, and procedural progress and does not necessarily contain personal information.

Germany, Ireland, and Spain have in comparison decentralised systems for storing participants' data. For example, in Ireland, data are stored by the intermediary bodies. Therefore, the databases and the information they contain are divided between the ESF programmes and according to the topics they cover. Similarly, in Spain, the system is decentralised to autonomous communities and regional authorities as they act as intermediary bodies. In Germany, the situation is further fragmented as participants' data can be stored internally by beneficiaries, at regional servers, and or by regional managing authorities without a coherent system throughout the country.

Table 5: Storing ESF participants' personal data per Member State

Storing ESF participants' personal data per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	Three interviewees mentioned that in the 2014-2020 programming period they store collected data in a database called ESF ZWIMOS, which is managed by the managing authority. It includes data that are relevant for both monitoring and evaluation and includes information about individual ESF participants. The managing authority is obliged by law to store data in this database.
France	Information about participants is stored centrally (nationally) in the Ma Démarche FSE database. In addition, each region has different systems, and some have databases similar to the national one.
Germany	Data storage does not seem to be harmonised. Data on participants can be stored internally by beneficiaries, at regional servers, and or by regional managing authorities according to interviewees. There are separate systems across the 17 managing authorities.
Ireland	Different databases are in use for storing participants' personal data. Databases in use differ among the intermediary bodies or operational programmes. One central database, the national e-cohesion system, is also in place to store all data securely.
Italy	One concrete example on how data is stored in Italy comes from the interview with the ESF beneficiary IAL FVG. They have their own internal digital management system, Ial Man, which records and makes available all data needed to implement the ESF projects. There are also regional and central databases where personal data regarding participants are stored.
Poland	Data are stored in a central database called SYRIUSZ, which is connected to several sub-databases such as the "SL" database. Participants' personal information is entered into these databases, which facilitates the process of verifying data, tracking of participants, and avoiding double-counting.
Romania	n/a
Spain	According to the national managing authority UAFSE, all the managing authorities and evaluators, whether external or not, use the databases of the Public Employment Services and the Ministry of Education to report and inform on the employment and education situation of programme participants.
Sweden	One beneficiary mentioned that it stores data on internal servers and in their data system Dynamics. The data must be stored for a period of at least four years according to the managing authority's instructions. The managing authority's instructions specify that project data must be stored until the end of the year four years after receiving the final decision on payment for implementing the ESF project. The period can be extended due to legal proceedings or upon request from the European Commission. The managing authority will then inform about such changes in written form. Data shall be saved in original, attested copies, or

Storing ESF participants' personal data per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
	on approved data carriers such as a CD, USB, or hard drive. Moreover, data that have been transmitted to Statistics Sweden will be stored until the end of the programming period.

3.1.3. Transmitting participants' personal data

Based on the interviews, the nine countries (excluding Romania as there are no sufficient answers regarding transmission of participants' personal data) can be divided into two categories in relation to each other when it comes to the possibilities to transmit personal data about ESF participants: less restrictive and restrictive.

Austria, France, Poland, Sweden, and Italy have less restrictive rules in place for facilitating the transmission and use of participants' data between organisations to conduct monitoring and evaluations. What they have in common is that participants' personal data are transmitted in one form or another centrally and are accessible for monitoring and evaluation for both public authorities (such as ESF managing authorities) and external evaluators.

- In Austria, personal data regarding participants, including special categories of personal data, are collected directly by beneficiaries and transmitted from the beneficiaries to the Federal Ministry of Labour for the purpose of evaluation via the ESF ZWIMOS database which is managed by the managing authority and from which also evaluators can request data. Data are also transmitted directly from beneficiaries to other actors such as their cooperation partners in the ESF projects.

- In Italy, participants' personal data are collected directly and from other public datasets by beneficiaries. These data are transmitted to regional managing authorities, who forward data to the national monitoring system that the MEF IGRUE manages. Moreover, data are also transmitted to other public institutions such as the Italian National Institute of Statistics (ISTAT), the Bank of Italy, and the Italia Court of Auditors. Normally, data transmitted to evaluators are anonymised, but there are examples from the interviews of access to non-anonymised sub-samples of data.

- In Poland, the supervision and monitoring of the implementation of projects co-financed by the ESF is currently within the scope of responsibility of the Minister of Family and Social Policy. Each region is an administrator of a database that collects participants' data, which are consolidated into a country-wide database hosted by the Ministry of Funds and Regional Development (the managing authority). An external evaluator explained that they obtain data regarding participants mostly from regional authorities, via a database called SL.

- Statistics Sweden (SCB) is a central institution for processing personal data about ESF participants and has a data sharing agreement with the managing authority (the Swedish ESF Council) and Af, the mayor beneficiary. Data that are collected by beneficiaries and then transmitted to SCB must not be anonymised since it has confidentiality requirements. From SCB, the managing authority, other institutions and external evaluators can request aggregated and or anonymised microdata for the purpose of evaluating the ESF. An external evaluator interviewed also collects data directly from participants, e.g., via surveys and interviews.

- In France, beneficiaries collect personal data directly from participants and in some cases, also from an intermediary body to verify participants' jobseeker status and whether they are registered or not. These data are transmitted to a central database at regional level and to the national Ma Démarche FSE database that is managed by the managing authority. Through this database, both managing authorities and evaluators may access participants' data, in addition to data collection directly from participants.

The restrictive systems are seen in Ireland, Spain, and Germany and have in common the rather fragmented data sharing systems either horizontally and or vertically between public institutions:

- In Spain, data collection for the purpose of monitoring and evaluating ESF programmes is decentralised to autonomous communities and regional authorities as they act as intermediary bodies. These data are provided to the managing authority UAFSE in an aggregate format, excluding special categories of personal data. All the managing authorities and evaluators, whether external or not, use the databases of the Public Employment Services and the Ministry of Education to report and inform on the employment and education situation of programme participants. However, as data processing is relatively decentralised and the possibilities to access data differ between regions, access to useful data is restricted in some regions, and statistical institutes may not be allowed to process any personal data for ESF monitoring and evaluation purposes. For the national managing authority, the steps to obtain data for the purpose of monitoring or evaluation reports are usually surveys, interviews, and consultations during open processes.

- In Ireland, the system relies on data sharing agreements that are put in place. These agreements are set up with the intermediary bodies and beneficiaries allowing them to collect and transmit data on ESF indicators between each other and to the managing authority. Without such agreement, no data can be transmitted. However, there are few examples of concluded data sharing agreements in Ireland. In practice, beneficiaries collect personal data directly from participants and in some cases from the intermediary body. These data are then transferred to intermediary bodies and a national central database. The managing authority access only anonymised data.

- For Germany, three interviewees mentioned that participant data can be transmitted to the relevant managing authority, but only one beneficiary mentioned that these data are not anonymised. Moreover, two regional managing authorities and the federal managing authority stated that they process only aggregated data. Some regional managing authorities may transmit these data to evaluators and other public authorities. However, different regions have different rules and practices in place regarding the processing of participants' personal data. Thus, there are challenges regarding accessing data centrally for the national managing authority and external evaluators.

Beneficiaries' transmission of personal data regarding participants

Table 6 shows an overview of how beneficiaries transmit ESF participants' personal data per Member State included in this study, according to interviewees. In Austria, France, Germany, Poland, and Sweden, interviewees stated that beneficiaries transmit personal data regarding participants to managing authorities (in Germany, three managing authorities stated that they access only anonymised data). In Poland, via specific regional and central databases that process participants' personal data, and in Sweden, via

Statistics Sweden, that transmits these anonymised data to the managing authority. One beneficiary in Sweden also mentioned that the managing authority may access (only view and not store) participants' personal data, but only samples for monitoring purposes. Moreover, in Ireland and Spain, interviewees stated that beneficiaries transmit personal data regarding participants to intermediary bodies. The managing authorities may access these data but only anonymised. Data may also be transmitted to other organisations such as to sub-contractors (according to an interviewee in France), or cooperation partners for further training purposes and to the apprenticeship office of the Chamber of Commerce (according to an interviewee in Austria).

Table 6: Beneficiaries' transmission of personal data regarding participants per Member State

Beneficiaries' transmission of personal data regarding participants. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	To cooperation partners for further training purposes (for planning and organising courses) and to the apprenticeship office of the Chamber of Commerce (for registering participants for qualification check). Also, data are transmitted to the ESF managing authority.
France	To the managing authority and in some cases, to sub-contractors.
Germany	To the authority who provides the funding and to regional managing authorities. However, the regional managing authorities in the regions North Rhine-Westphalia and Brandenburg and the federal managing authority stated that they process only aggregated data.
Ireland	To a national central database and intermediary bodies.
Italy	In the FVG region, to regional authorities for monitoring and reporting purposes, and the implementing party of the funding.
Poland	To a database called Syrius, which is a database that is managed by the Ministry of Labour. Participants' personal data is also transmitted to a separate database called SL, managed by regional authorities, which is integrated with Syrius, to enabling tracking of participants in different projects. The managing authority also consolidates the data in the Syrius database. The managing authority is required to establish a system to record (i.e., collect and enter) and store data in computerised form on each operation necessary for monitoring and evaluation, including data on individual participants in operations, where applicable.
Romania	n/a
Spain	To intermediary bodies, who transmit aggregated data to the managing authority. Data are used for both monitoring and evaluation. According to a national managing authority, no special categories of personal data are processed.
Sweden	To the managing authority via a "consolidation report" in an Excel sheet according to a template provided by the managing authority. The template includes information on name, social security number, employment status, qualifications achieved, and participation in ESF activities. This information is reported to the managing authority every month via SCB according to the same procedures that apply to all ESF beneficiaries. SCB receives non-anonymised data, but when it transmits data to the managing authority or evaluators, the data is always anonymised (anonymised microdata). According to one beneficiary, the managing authority has the right to access (only view and not store) participants' personal data but only samples for monitoring purposes.

External evaluators' collection of personal data regarding participants

Table 7 shows how external evaluators collect ESF participants' personal data per Member State included in this study, according to interviewees. In France, Germany, Italy, Poland, Spain, and Sweden, interviewees mentioned that external evaluators have accessed data regarding participants from the managing authorities. In Austria, France, and Poland, such data were accessed through regional and or national databases, whereas in Sweden, through SCB. Out of these, interviewees in Italy and Sweden stated that such data are usually anonymised. However, for one evaluation in Italy, sub-samples of personal data were accessed by the evaluator, and one evaluator in Sweden stated that it could at least access contact details for participants from the managing authority and beneficiaries on several occasions. Moreover, in Austria, one interviewee gave the information that the Austrian data protection authority did not allow the transmission of participants' national insurance numbers to evaluators. Other data collection methods such as interviews and surveys to gather personal data directly from participants are also in use by the evaluators, as stated by interviewees in Germany, Spain, and Sweden.

Table 7: External evaluators' collection of data regarding participants per Member State

Information from interviewees – External evaluators' collection of data regarding participants. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	According to the managing authority, the Austrian data protection authority did not allow the transmission of participants' national insurance numbers to evaluators during the ESF 2014-2020 period. It remains to be seen if the processing of participants' social security numbers will be possible during the ESF+ period 2021-2027.
France	From the national database MaDémarcheFse that is managed by the managing authority and similar regional databases upon agreement with the managing authority, including special categories of personal data.
Germany	One research institute stated that it can access monitoring data from the managing authority (project data and participants' data). The research institute also collects data from participants via its own surveys.
Ireland	n/a
Italy	According to the Le March Region managing authority, it transmitted anonymised data in the evaluation phase to the evaluator. All the data linking was done by regional offices. Just for one evaluation that required detailed processing of data, non-anonymised sub-samples of data were transmitted.
Poland	One evaluator uses data obtained from a database called SL, which holds data concerning ESF participants. This database include data that are transmitted by beneficiaries and is administered by regional authorities and consolidated by the managing authority.
Romania	n/a
Spain	From managing authorities. According to one evaluator, only anonymised data, excluding special categories of personal data. System, operational or thematic evaluations are normally carried out externally under the supervision of the managing authority. The methodology for obtaining data is indicated in each evaluation, although the starting point is usually through interviews and surveys with each intermediary body and/or beneficiary.

Information from interviewees – External evaluators' collection of data regarding participants. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Sweden	According to one evaluator, data used to evaluate ESF are combinations of surveys, interviews, document studies, desk research, literature reviews, and statistical analyses of statistics received from the managing authority and Statistics Sweden. From Statistics Sweden, the evaluator gets aggregated data. The managing authority transmits only aggregated data. One evaluator has accessed data such as contact details of project participants, organisations, and project leaders. Data is mainly related to project indicators. Most assessments from the previous two years involved qualitative data and surveys. If this evaluator cannot gain access to contact details from the managing authority or other organisations, the link to the survey is instead sent to beneficiaries / project managers who can forward the link to the participants. Also, project managers might send contact details upon the evaluators request that explains the purpose, and after consent from the contact persons.

Box 1: Key findings - Processing of ESF participants' personal data

- Beneficiaries collect personal data directly from participants in all nine countries covered in this study according to interviewees. According to interviewees from Austria, France, Ireland, Poland, Germany, and Sweden, these data may include special categories of personal data.
- According to interviewees, Austria, France, Poland, and Sweden have centralised systems for storing personal data regarding participants. Apart from Sweden, where data are processed by SCB, these databases are managed by the managing authority. In Italy, data storage is divided between the national and regional levels that may contain different types of data. In Germany, Ireland, and Spain data are stored decentrally. In Ireland and Spain mainly by the intermediary bodies as the highest level, and in Germany, different systems apply in the different regions.
- Access to personal data regarding participants differs among the stakeholders interviewed per Member State. In Germany, Ireland, Spain, and Sweden, interviewees stated that managing authorities may access only anonymised or aggregated data (in Sweden, only viewing samples of data for control checks).
- In France, Germany, Italy, Poland, Spain, and Sweden, interviewees mentioned that external evaluators have accessed data regarding participants from the managing authorities. In Austria, France, and Poland, such data were accessed through regional and or national databases, whereas in Sweden, through SCB. Out of these, interviewees in Italy and Sweden stated that such data are usually anonymised.
- Instead of access to previously collected personal data regarding participants, it is a practice among the nine countries that managing authorities (France and Spain) or evaluators (Germany, Spain, and Sweden) collect data directly from participants via surveys and/or interviews.

3.2. Accessing administrative data for the purposes of monitoring and evaluation of the ESF

Interviewees from all nine Member States indicated that administrative data are used for both monitoring and evaluation purposes, although in Germany and France, it is done to a limited extent according to interviewees.

From looking at Table 8 on the number of administrative data types and datasets that are in use for monitoring and evaluating ESF in each Member State mentioned by the interviewees, France and Germany stands out for having restrictive rules for access to administrative data. In Ireland, administrative data is used frequently. However, the data are seldom shared between institutions. In Ireland, the intermediary bodies are also administrative data holders. Thus, they have access to their own data for monitoring and evaluation purposes. These can only be transmitted if a data sharing agreement is in place, which according to the Irish managing authority are rare and a lengthy process to conclude. Only one example exists in Ireland relevant for the ESF, the Jobseekers Longitudinal Dataset (JLD), which draws together payment and administrative data from the Department of Social Protection and data from SOLAS and the Revenue Commissioners. In Austria, the managing authority stated that administrative data were used for evaluation purposes alone, in two counterfactual impact analyses. It also plans to use administrative data for evaluation purposes in the ESF+ programming period – employment, income, and school data. In Sweden, administrative data are managed centrally by SCB for ESF purposes. It can link different datasets and ESF monitoring data but transmits them to the managing authority and evaluators anonymised data. In Italy, administrative data are accessible, despite not having a fully centralised system. Interviewees from different stakeholder types, including beneficiaries and several managing authorities stated that they use administrative data from several databases for both monitoring and evaluation. In Spain, interviewees among beneficiaries, a managing authority, an evaluator, and the Data Protection Authority clarified that administrative data are often used for both monitoring and evaluation. Also in Romania, a beneficiary and a managing authority stated that administrative data are used, both for monitoring and evaluations.

In Romania, the interviewee from the National Statistical Institute stated that its personal data are confidential if the data subjects are identifiable. This confidentiality rule is regulated by the data protection law and Law 226/2009 on the organisation and operation of official statistics in Romania. Moreover, in Spain, the Statistical Institute of the Region of Valencia explained that the regional statistical institutes in Spain (with the exception of Catalonia and the Basque Country) work with fully anonymised data from the National Statistics Institute. The interviewee from the statistical institute of the Basque Country (Eustat) stated that the data protection legislation is excessively strict for statistical purposes since Eustat cannot process any kind of personal data to carry out ESF evaluations. Eustat has processed minimal personal data to publish statistics (previously anonymised). However, it has recently been sanctioned by the Basque Agency for Data Protection with a warning, in this case, for failing to comply with the current LOPDGDD[26]. Eustat has appealed the sanction before the Superior Tribunal of Justice of the Basque Country. Moreover, data sharing agreements between public institutions are common among most of the nine countries. However, these agreements might be complex to conclude, and if the access to administrative data is not centralised, such agreements might be additionally complex to conclude with the multiple actors involved.

[26] Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales - LOPDGDD (Organic Law 3/2018 on the Protection of Personal Data and the guarantee of digital rights).

Given the information above and in Table 8 below, it can be observed that only Sweden has a more centralised systems for access to administrative data than the rest of the nine countries. In Sweden, administrative data are accessed centrally from SCB.

The other Member States have more diverse systems for the processing of administrative data for monitoring and evaluation of the ESF:

- In Austria, administrative data are not necessarily accessed from a single source. However, for ESF monitoring and evaluation purposes the facilitation for access is partly managed centrally by the managing authority.

- In France, based on the information received by the interviewees, data are gathered partly from the national MaDémarcheFSE database, and partly from regional databases, through managing authorities. However, these data concern data collected regarding ESF participants. The information given by the French Data Protection Supervisory Authority indicated that certain persons at the different public institutions have access to administrative data, respectively. Thus, processing of administrative data in France for ESF monitoring and evaluation cannot be described as centralised.

- In Germany, different rules and datasets are applicable among the different regions. No harmonised central system can be detected given the information from the interviewees.

- In Ireland, the processing of administrative data for ESF monitoring and evaluation is restricted to the individual intermediary bodies that also host administrative data. However, there is one relevant data sharing agreement in place that enables the transmission of administrative data between public institutions for ESF monitoring and evaluation purposes.

- In Italy, processing of administrative data is not fully centralised. The managing authority at national level and at regional level described different procedures and access points.

- In Poland, processing of administrative data is not fully centralised. While the transmission and storage of participants' personal data are harmonised within the country, different administrative datasets have been used and the ways to access these have differed depending on the actor.

- In Romania, no centralised or harmonised system was described.

- In Spain, no centralised or harmonised system was described.

Table 8: Use and transmission of administrative data per Member State

Use and transmission of administrative data per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	Data on employment status, income, and social benefits are used for both monitoring and evaluation purposes. The process of transmitting administrative data for ESF evaluation purposes is partly managed centrally by the managing authority BMAW. For evaluations and impact analyses, evaluators must request data from the ZWIMOS database through BMAW and link and compare it with data from the AMS-DWH (Public Employment Service Data

Use and transmission of administrative data per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
	Warehouse) database. Pseudo-anonymisation is done via an external service provider. The managing authority stated that administrative data is not used for monitoring purposes. However, it plans to use it for the ESF+ programming period, but only for indicator EECR05: employment status from social security register. One evaluator interviewed stated that it only uses data that are collected directly from participants and transmitted via the ZWIMOS database. The managing authority stated that administrative data were used for evaluation purposes alone for two counterfactual impact analyses. However, certain restrictions exist such as the use of national insurance numbers. For the ESF+ programming period, it also plans to use employment, income, and school data.
France	Among the interviewees, only one actor, an external evaluator, stated that it uses administrative data for evaluation purposes. It referred to data from the MaDémarcheFSE database at the national level that has data on ESF participants. The information included what is necessary for the survey that the evaluator carries out six months after the project, including phone number, e-mail address, address, employment status, and integration rate of disadvantaged persons. Moreover, the regional managing authority in Normandy, stated that it uses administrative data for monitoring purposes, including information from participants' ID cards, and employment status. Information is accessed from the MaDémarcheFSE database. The national managing authority does not use administrative data.
Germany	One regional managing authority stated that it uses administrative data for monitoring purposes. However, it specified that these data are anonymised. It concerns data on socio-economic framework conditions to contextualise programmes, forming comparison groups, and shares of participants with a migrant background. Neither of the other managing authorities stated that they use administrative data for monitoring or evaluation. However, the federal managing authority stated that for one evaluation, it facilitated access to administrative data to one external evaluator for an evaluation. These data included long-term indicators regarding ESF participants' employment status from the federal employment agency. The federal managing authority is legally not allowed to access these data according to the interviewee. Moreover, the regional managing authority in Brandenburg stated that it has an interest in using administrative data but can currently only access anonymised data. A similar answer was given by the managing authority in North Rhine-Westphalia, i.e., that it has access to statistics and anonymised data for evaluation and monitoring purposes. The research institute interviewed stated that it has used only monitoring data of the managing authority, i.e., project- and participants' data. One related difficulty regarding access to administrative data concerns the different procedures depending on the government level of the data, and which legal provisions apply to the specific dataset.
Ireland	Several administrative data sources are used such as on social protection payments, employment registers, pension registers, a joint database from education and training, and several other sources for higher education. These are used both for monitoring and evaluation purposes, including special categories of personal data, but anonymised. One database that integrates several datasets is the JLD that is managed by the Department of Social protection and shared with SOLAS (a state agency for the further education and training sector) and the Revenue Commissioners. Also, other databases are held by different authorities and intermediary bodies. Although administrative data are used, they are hard to get hold of, especially between public authorities. Intermediaries use mostly administrative data from their own datasets. Data sharing agreements must be in place to enable transmission of administrative data. According to the Irish managing authority, data sharing agreements are rare and lengthy processes to conclude in Ireland.. The JLD draws together payment and administrative data from intermediary bodies and has previously been used for ESF evaluation. It contains information on a claimant's sex, age, marital status, nationality, educational attainment, previous occupation, employment and unemployment history (duration and number of episodes), unemployment training history (type, duration and number of episodes), benefit type, spousal earnings (to qualify for an adult dependent allowance), number of child dependents, family payment type (i.e., adult and child dependent allowances, adult only, etc.) and geographic location. Through the development of the JLD, administrative data events are

Use and transmission of administrative data per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
	linked to episodes of welfare or work, thus enabling the better ex ante and ex post analysis of jobseekers.
Italy	Administrative data are frequently used for monitoring and evaluation purposes. For example, employment data regarding participants, and tax, police, and court records regarding beneficiaries. Also, data from the COMarche dataset that include information on sex, age, education, citizenship, and employment history are used. The managing authority ANPAL has special agreements in place according to data protection rules to access the administrative data required from other public institutions. Also, at a regional level, the managing authority of the Marche Region can gain access to several administrative datasets, both for monitoring and evaluation purposes. For external evaluators, data may be provided anonymised, but not always. If the data comes non-anonymised, it is followed by privacy rule protocols, and may include only sub-samples of variables according to one interviewee.
Poland	Data from the SYRIUSZ system is used to monitor participants in ESF-funded projects implemented by the Public Employment Services. This is an ICT system supporting the implementation of the statutory tasks of poviat labour offices (PUPsa). Data on participants in projects implemented by PUPs, i.e., in the area of the labour market, are exported to the ICT system for ESF 2014-2020 monitoring. The SYRIUSZ system collects data on the clients of the PUP, including, inter alia, their age, experience, education, the support provided to them and its temporal scope, or the expenses related to the support, as well as the labour market status of the person receiving support. It is possible to retrieve information from the register in terms of voivodeship, poviat, commune, township, and street. It is a defined database, from which the downloaded data categories are selected at later stages to complete the data of ESF project participants. In order to calculate the value of long-term result indicators first of all, data coming from the records of the Social Insurance Agency (ZUS) concerning paid contributions (codes of insurance titles to which a given person is subject and the assessment basis for calculation of the amount of health and accident insurance contribution) are used. In case of evaluation relating to support from the Operational Programme Knowledge, Education and Development, data on the results of external examinations collected by the Central Examination Commission were also used. Administrative data are stored by the individual institutions holding the data, both nationally and regionally. To access data from the Social Insurance Agency, the Ministry of Funds and Regional Development has to sign a special agreement. In general, such agreements are necessary to access administrative data from different institutions. At a regional level, the Employment Office of the Capital City of Warsaw must have a special legal basis for accessing data from the regional administrative employment office.
Romania	One beneficiary most frequently used data from the national Institute of Statistics, Ministry of Education, Ministry of Internal Affairs, and Police records. For monitoring purposes, one managing authority mentioned that administrative data are in use, including data from the following sources: • Persons Record (identification data); • General Registry of Employees, Labour Inspection; • National Agency for Fiscal Administration (income, social contributions); • National Agency for Unemployment – beneficiaries of public employment services, including information on trainings performed within the Unemployment Agency; • National House of Public Pensions; • Trade Register Office – for information on legal persons; • National Agency for Social Benefits – for the minimum social income. For evaluation purposes, the managing authority stated that administrative data are in use, including on employment status, job seekers, and beneficiaries utilising unemployment

Use and transmission of administrative data per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
	services, including training. Administrative data are stored by the individual institutions holding the data. In general, to access data, one must define the purpose. The procedure for gaining access would differ depending on the processing purpose and the category of personal data. To access personal data, an institution needs to comply with the following requirements: • be an authorised institution that can work with personal data; • have a clear legal provision regarding the legal right to access that information; • have a clear protocol between the institution that provides the administrative data and the institution that request access; and • clearly define the persons that have the right to use that data. One certain restriction is that the National Institute of Statistics is not allowed to share any administrative data. The interviewee from the National Statistical Institute stated that its data are confidential if personal data are identifiable. Such confidentiality is regulated by the data protection law and Law 226/2009 on the organisation and operation of official statistics in Romania.
Spain	Administrative data used include data from the national Tax Administration Agency regarding, e.g., date of birth and economic situation, and social security registers for information regarding possible vulnerable situations such as social service programmes situations of gender-based violence. Data such as public register data (births, marriages, and deaths), immigration records, employment status, school or education records, social services records, and data from the Spanish social security health system could also be used. Administrative data are stored by the individual institutions holding the data. To access administrative data for the purpose of monitoring and evaluating ESF programmes, the interested party must comply with certain legal criteria and security requirements. In Spain, the statistical institutes interviewed stated that they cannot transmit personal data.
Sweden	Administrative data in use include data on gender, age, country of birth, data from the population register, and level of education. Also, data from the Swedish Public Employment Service on unemployment, and on reduced work capacity due to disabilities, and newcomer immigrants are used. Information on paid student grants can be obtained from the Swedish Board of Student Finance. In some cases, information on activity compensation and sickness benefit can be obtained from the Swedish Social Insurance Agency. Administrative data used are also e.g., employment records to assess effects of projects, including background data, employment rate, and transition between studies and work. Just as all participants' data are reported to SCB, administrative data are accessed through SCB, to which other public authorities share their administrative data. The ESF managing authority, beneficiaries, and external evaluators can thereafter access administrative data from SCB for both monitoring and evaluation purposes. To facilitate access to these datasets, it helps if the requests are as specific as possible in terms of objective and scope. With this system, different data records can be linked, also with ESF participants' personal data.

Box 2: Key findings - Processing of administrative data

- Administrative data are used for both ESF monitoring and evaluation in all nine Member States, although to a limited extent in Germany and France according to the interviewees.

- In comparison to the other Member States, Sweden has a centralised system for accessing administrative data for ESF monitoring and evaluation.
- Interviewees from statistical institutes in Romania and Spain expressed that the rules concerning transmission of administrative data by these institutes are restricted to anonymised data. Also in Sweden, the national statistical institute cannot transmit non-anonymised data.
- Data sharing agreements are used to process administrative data.

3.3. Main challenges

As shown in Table 9 below, the main challenges mentioned by stakeholders can be summarised as follows.

- Gaining access to administrative data can be time consuming and there might be a long waiting time after a request has been made (as mentioned by interviewees in Austria, Ireland, Poland, Spain, and Sweden). In Germany, access to administrative data is very limited.
- Heavy costs involved to access administrative data, because the organisations, especially external evaluators, might need to buy data from the data holders (challenges due to costs was mentioned by interviewees in Austria, Poland, Romania, and Sweden).
- Complex processes to conclude data sharing agreements (as mentioned by interviewees in Ireland and Poland).
- Decentralisation and fragmentation between levels of government and horizontally between regions (concerns mainly Germany).
- Interoperability challenges between data sources including between different information systems and between regions and national level data (as mentioned by interviewees in Germany, Ireland, Italy, Poland, Romania, and Spain).
- Requirements laid down for the protection of personal data (at the national level?), especially regarding the use of special categories of personal data (as mentioned by interviewees in Germany, Ireland, and Spain).
- Lack of prior consent from data subjects to share data (as mentioned by interviewees in Germany and Ireland).
- Certain restrictive rules for statistical institutes (as mentioned by interviewees in Romania and Spain).

Table 9: Main challenges per Member State

Main challenges per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	• Time-consuming to make data usable, to request administrative data and to anonymise them (the whole process must involve multiple actors). There are also high monetary costs involved. • It is hard to get information on whether participants have qualified or not to participate in the ESF projects.
France	• When the beneficiary wants to verify the jobseeker status of ESF participants, it sometimes asks for proof to "Pole Emploi" to ensure that the person is indeed registered as a jobseeker. Pole Emploi has refused the last requests for documents with arguments related to GDPR (which was not further specified by the interviewee). Also, lack of knowledge regarding which types of data beneficiaries can collect and about safe transmission methods.
Germany	• Decentralised data processing and fragmented storage depending on the level of government, i.e., the federal, regional, and local levels. • The ESF/ESF+ managing authorities are not allowed to access personal data or administrative data for data protection reasons. Only research institutes and selected authorities may do so. • Unavailable data as some special categories of personal data, i.e., regarding minorities and disabilities are not collected in Germany according to interviewees. • There is a lack of understanding of data protection rules, which are fragmented between levels of government. • Datasets are not always interoperable. • There might be no prior consent from participants to transmit data, and the bureaucratic burden to ask for consent is heavy.
Ireland	• Difficulties regarding concluding data sharing agreements. According to the Irish managing authority, data sharing agreements are rare and lengthy processes to conclude in Ireland. Only one example exists in Ireland relevant for the ESF. • Uncertainties concerning how to interpret data protection laws and what applies specifically to ESF and the mandate per institution. In general, individual officials may be afraid to break data protection rules. • The Higher Education Authority (HEA) said they cannot collect special categories of personal data. • Time consuming to access data. • No predefined indicators and since they must include indicators from what beneficiaries should collect, they cannot get data on those indicators.
Italy	• It is not always possible to access complete datasets requested. • It may be challenging to comply with EU and national data protection legislation, especially data processing regarding GDPR Articles 9 and 10. • Lack of interoperability between different information systems and between regions and national level data.
Poland	• Legal restrictions, time-consuming procedures, and lack of interoperability of data systems. The Ministry of Funds and Regional Development mentioned that it can take several years to conclude data sharing agreements to facilitate access to administrative data. In addition, it can be costly and time-consuming to extract data from registers and adapt IT systems to process the data.

Main challenges per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Romania	• Restricted access to data on education (handled by the Ministry of Education) to evaluate the ESF, due to insufficient clarification according to an interviewee at a managing authority on the legal basis for processing such information. It is hard to interpret the existing laws in Romania and the operators (institutions that exchange data) want legislation that establishes unequivocally that they can exchange data in accordance with the GDPR, according to one interviewee. • Legal bases for processing of personal data (Article 6 of the GDPR) require better regulation in Romania, according to one interviewee. • Lack of transparency, lack of collaboration between institutions, and lack of coherent procedures and regulations. • The cost to access data can be an issue.
Spain	• Lack of data and time-consuming processes to access existing data. • A lack of interoperability between administrative data holders and regions, which creates inefficiency in data processing. • The lack of existing data due to public authorities' inability to collect data. • According to the managing authority, no special categories of personal data or microdata can be processed for ESF monitoring and evaluation, which was indicated as a challenge by the interviewee. Data protection legislation is very strict in Spain regarding data for statistical purposes. Public statistical institutes in Spain such as Eustat have access to multiple types of data from different sources. However, they are not allowed to use all or share them due to national data protection legislation and statistical secrecy rules and cannot process them for ESF purposes.
Sweden	• Regarding collection of data from ESF participants, challenges may include data subjects' willingness to give their consent to the processing of their personal data when confirmation of the data subjects' consent is required for the beneficiary to collect information regarding ESF indicators. However, it is very rate that someone does not want to give their consent. • Challenges regarding access to administrative data may concern waiting time and costs involved to access data from SCB.

3.4. Potential solutions/good practices

In accordance with Table 10 below, the main solutions suggested can be summarised as follows.

- The use of unique identifiers.
- Better data processing coherence between regions and levels of government and better interoperability between the systems.
- Harmonised data protection laws horizontally and vertically (regarding Germany, as a federal state).
- Instead of using (explicit) consent for the collection of personal data, consider using other available legal bases such as "public interest" or "legal obligation".
- Data protection contact points for ESF.

- Clearer definition of data collection purposes to facilitate collection, including early defined monitoring and evaluation indicators.

According to an interviewee in Italy, certain data protection restrictions might be overcome through a data protection impact assessment pursuant to Article 36 of the GDPR and a possible consultation with the national DPA.

Table 10: Examples of potential solutions per Member State

Suggestions of potential solutions per Member State indicated by interviewees. Note that the solutions suggested in this table may not yet been implemented, unless it is stated. (Note also that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	• Linking personal data through a unique number to facilitate access and easier linking of data.
France	n/a
Germany	• Regarding the new ESF+ funding phase 2021-2027, an interviewee at a regional managing authority mentioned that it had a discussion with its data protection officer and held several workshops on the processing of personal data. Based on these, one idea is to look at which data the Ministry has a legal basis for, so that participants need only to be informed, rather than having to actively agree with data protection guidelines. Moreover, an interviewee from the federal managing authority mentioned a recommended method of 'informed estimates' (fundierte Schaetzung) to estimate indicator values on participants as an alternative solution to receive otherwise missing data, without participants' consent, has been denied by national authorities in Germany with the argument that one cannot preclude that an informed estimate of a characteristic may represent personal data in an individual case. It concerns special categories of personal data, such as regarding ethnic minorities and disabilities.
Ireland	• When working on the European Globalisation Adjustment Fund (EGF) regarding unemployed workers, the managing authority PEIL was able to get data on employment updates every four months from the Revenue Commissioners to meet EGF reporting requirements, which is not as detailed as ESF reporting requirements. • During the programme, the data protection advisors of the intermediary bodies suggested that the collection of data should be based on a legal obligation or a significant public interest to process data. • A data protection contact point for the ESF would be useful. • Within the Erasmus programme, there are very useful guidelines on data processing and GDPR, which can be seen as a good example.
Italy	• Certain data protection restrictions might be overcome through a data protection impact assessment pursuant to Article 36 of the GDPR and a possible consultation with the national DPA.
Poland	• Increased legal flexibilities for the application, use, and transmission of administrative data between public authorities.
Romania	• Better description of data processing purposes can facilitate the process of gaining access to administrative data.

Suggestions of potential solutions per Member State indicated by interviewees. Note that the solutions suggested in this table may not yet been implemented, unless it is stated. (Note also that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
	• It would be useful to elaborate clear eligibility rules, so it is no longer necessary to verify the entire documentation containing personal data.
Spain	• Greater data processing coherence between regions and levels of government and better interoperability between the systems. Access to the Spanish Government's Data Intermediation Platform would facilitate greater interoperability. • To facilitate evaluations, public register data should be linked to tax register data such as income level. • One good practice regarding the use of administrative data for evaluations was mentioned: in the context of the Youth Guarantee (co-financed by the ESF), an agreement was made between the Administrative Unit for the European Social Fund (UAFSE) with a relevant Spanish consultancy. Another good practice mentioned concerned Catalonia, which has procedures to expedite information to consultancies, which can be considered a highly relevant procedure comparable to good practices in Spain. • According to an interviewee at the Mancomunidad Intermunicipal Alto Palancia, access to the vast majority of administrative data (economic, social, family, etc.) requires the data subject's consent. This is a restriction or challenge. To meet this challenge, the interviewee suggested asking the data subjects for consent in advance so that they can process the files in time. The county council should provide more data protection guidance. • For statistical institutions, it would be convenient to differentiate between public purposes (of any type of administration) and private ones instead of statistical and research purposes to reduce widespread restrictions on the processing of personal data.
Sweden	• Since paying consultancy companies to get legal advice is expensive, it would be better if the Swedish ESF Council could have data protection expertise available to beneficiaries. • According to the beneficiary Af, they were previously processing data on the basis of data subjects' consent even though there is a legal obligation (based on Swedish law) which makes it necessary to process personal data. The beneficiary recently changed its legal interpretation and does not seek data subjects' consent anymore to process and transmit their data. However, according to the interviewee, it would be even better if there was a law that stipulates concretely that the specific beneficiary must process data for ESF purposes.

3.5. Guidance/advice

Table 11 shows advice received regarding data protection issues per Member State included in this study, according to interviewees. Among the nine Member States, only one interviewee from Romania mentioned advice given from their national DPA. The French DPA (CNIL) said that they have been contacted several times regarding data collected from participants but not regarding administrative data. Instead, the actors interviewed seek advice from in-house Data Protection Officers (DPO) or equivalent, contracted experts, ESF intermediary bodies or managing authorities. The advice they need and have received is very diverse. However, a common need is to bring clarity in how to comply with data protection laws, which rules apply and how to interpret them. Also, regarding efficient ways to ask for data subjects' consent and when it is necessary, and on which legal basis lawful data processing can be based need to be clarified.

Table 11: Advice received regarding data protection issues per Member State

Advice received regarding data protection issues per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Austria	No advice has been given by the Data Protection Authority. Instead, the organisations interviewed receive internal advice from DPOs or similar. One interviewee mentioned that more advice is needed regarding consent practices whether consent is needed and whether ESF's legal framework provides the legal basis needed to collect some data such as special categories of personal data.
France	All interviewees mentioned that they have received advice in one way or another, but not from the French DPA (CNIL). Instead, advice has been received from in-house, contracted specialists, or from the managing authority. The CNIL said that they have been contacted several times regarding data collected from participants but not regarding administrative data. In its general advice, the CNIL has recalled that only data relevant to the purpose of the processing operation could be transmitted regarding the ESF and made recommendations not to process certain categories of data which did not seem useful for the projects referred to it. It also questioned the precision, objectivity and appropriateness of certain terms used (e.g., the statistical definition of persons of foreign origin), as well as the legality of collecting certain data (membership of 'ethnic minorities') under French law. In this regard, it recommended that only objectively definable categories of data be used (e.g., commune of birth and nationality of parents).
Germany	Data protection advice is received mostly through internal advisors and training. For example, the North Rhine-Westphalia managing authority had discussions with its DPO, held workshops, and discussed legal solutions for the 2021-2027 funding period. Based on these, one idea was to look at which data the Ministry has a legal basis for, so that participants need only be informed, rather than having to actively agree with data protection guidelines.
Ireland	Advice is received mostly from in-house DPOs or from intermediary bodies and auditors. In addition, the government's legal team (Chief State Solicitor's Office), the Attorney General's office has given advice on data sharing agreements regarding processing ESF participants' data but not on the use of administrative records. They advised to seek explicit consent. However, the data protection advisors of the intermediary bodies suggested instead that the collection of data should be based on the legal obligation (Article 6(1)(c) GDPR) or a significant public interest (Article 6(1)(e) GDPR) to process data.
Italy	The Italian interviewees did not mention much regarding data protection advice, and when advice is given, it generally comes internally. Also, The Italian DPA has not formally provided any guidance regarding ESF or carried out any investigation. However, the authority has been in contact with several national authorities and the EDPB regarding transmission of ESF beneficiaries' personal data.
Poland	No interviewee has received any advice from the Polish DPA. This is confirmed by the DPA, who has had no interaction regarding ESF-related matters. Instead, the actors interviewed make use of either internal DPOs or contract external companies for data protection advice.
Romania	The interviewee from the National Unemployment Agency was the only one who stated having received advice from the national DPA. To get advice, the agency requested the DPA's view on processing information related to education regarding the possibility of concluding a protocol with the Ministry of Education for communicating such data to the Unemployment Agency. The DPA replied that the Romanian legislation must be aligned to the requirements under the GDPR and, thus, clarify the legal basis for communicating information regarding education to the Unemployment Agency. Thus, a protocol cannot constitute a legal basis for data processing. Moreover, the Unemployment Agency would need additional advice and clarification on the legal basis and purpose of processing personal data for administrative purposes. Moreover, the interviewee of the National Data Protection Supervisory Authority responded that it has frequently provided guidance and opinions to public authorities, but not specifically regarding the ESF.

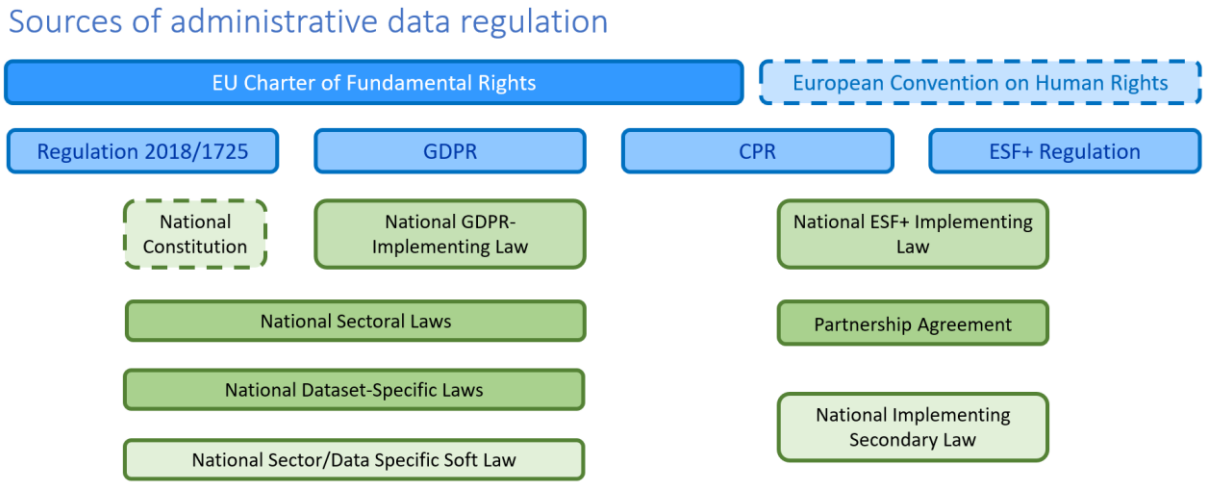
Advice received regarding data protection issues per Member State. (Note that this table only displays information that has been stated during interviews held for the purpose of this study. Other practices might apply per Member State.)	
Spain	No guidance from any DPAs exists. Several interviewees stated that specific guidance would be useful, both nationally from the AEPD and regionally from regional DPAs. Since the Valencian Community has no regional DPA, the Valencian Statistical Institute relies on the AEPD. The Valencian Statistical Institute believes that the AEPD should implement more instructions and guidelines to create a greater typology of data in coherence with data protection regulations to facilitate more precise and reliable statistics.
Sweden	Most interviewees get advice internally and in dialogue with the managing authority. One beneficiary got external expertise from consultancy companies on GDPR-related issues but not connected to ESF specifically. This advice has been related to the practice that employers share personal data about their employees, who are ESF participants, before receiving consent from the employees. The conclusion was that this is legally possible because the beneficiary is obliged to report information on participants for whom it receives funding.

4. Description of the legal framework

This Section provides an overview of the legal framework applying to personal data relevant to the ESF+ monitoring and evaluation. These data include data collected directly from participants (such as data collected in surveys), participants' personal data from administrative registers, and non-participants' data, for instance in the case of counter-factual analysis for evaluation purposes.

The Figure 1 below provides an overview of the different sources of administrative data regulation, both at EU and national level. These sources will be presented in this Section, highlighting those elements that are particularly useful in the context of the ESF+ monitoring and evaluation.

Figure 1: Sources of administrative data regulation



The first Sub-section will present the general EU legal framework regarding data protection relevant to the processing of data related to the ESF+ monitoring and evaluation. The second Sub-section will describe the legal framework of nine selected Member States, by identifying their GDPR-implementing law, the legislation implementing the CPR 2021 and the ESF+ Regulation, the courts with jurisdiction over data protection cases and their DPAs.

4.1. Description of the EU level legal framework that has data protection implications for the monitoring and evaluation of the ESF+

EU primary legislation contains provisions on data protection in the EU which are found in several different legal instruments. First, the right to protection of personal data is laid down in **Article 16(1) of the Treaty on the Functioning of the EU** (TFEU)[27]. Additionally, **Article 8 of the Charter of Fundamental Rights of the European Union** (EU Charter), which has the same legal value as the EU Treaties[28], enshrines the right to protection of personal data and stresses that the processing of such data must be fair, for specific purposes, have a legitimate legal basis and that compliance with these requirements must be subject to control by an independent authority[29]. This right is closely linked to Article 7 of the EU Charter which recognises the right to respect for private and family life. Article 52 of the Charter on the scope and interpretation of rights and principles entails a detailed balancing test for interfering with fundamental rights, including on the right to data protection, as further elaborated by the Court of Justice of the EU[30]. Compliance with the provisions of the EU Charter for operations selected and implemented under the ESF+ Regulation is underlined in Article 8 of the latter Regulation[31].

The case law of the **CJEU** is to be considered in order to identify legal principles established by the Court and better grasp the rules to be taken into account in the processing of personal data for the purpose of ESF/ESF+ monitoring and evaluation. In some of its judgments, the Court gives guidance on the processing of data on the legal bases of Article 6(1)(c) and (e) – legal obligation of the controller and public interest. For instance, in a recent case, the CJEU confirmed that processing on the basis of a legal obligation should be based on a national or EU legal provision and be proportionate to the interest pursued[32]. Whilst Lithuanian law obliges companies receiving EU funds to publish online declarations of private interests of individuals, who do not hold public roles, the Court said that this obligation did not pass the proportionality requirement. Moreover, the Advocate General Bobek in his opinion on *SIA 'SS' v Valsts* considered that it is essential for an entity intending to process personal data to consider the **nature and the purpose of the processing from the very beginning**, i.e., the assessment of the lawfulness of the processing should be the first element of such a processing activity[33]. This opinion also stressed that data transfers and the type of transfer to a tax authority must be **clearly defined in the national provisions** established in accordance with Article 6(1)(c). Furthermore, where data processing based on Article 6(1)(e) is carried out by a public tax authority, the CJEU in the *Peter Puškár* case considered that the drawing up of a list of persons who are to be targeted by the authority must be **adequate and necessary** to reach the objectives, that there must

[27] Article 16(1), Treaty on the Functioning of the EU (TFEU).

[28] Article 6(1), Treaty on European Union (TEU).

[29] Article 8, Charter of Fundamental Rights of the European Union, (2012).

[30] See e.g. Joined Cases C-37/20 and C-601/20, Luxembourg Business Registers. ECLI:EU:C:2022:912, Court of Justice of the European Union, Judgment of the Court (Grand Chamber) 22 November 2022., para.45 et seq.

[31] Article 8, Regulation (EU) 2021/1057 of the European Parliament and of the Council of 24 June 2021 establishing the European Social Fund Plus (ESF+). (Hereinafter ESF+ Regulation).

[32] Vyriausioji tarnybinės etikos komisija, ECLI:EU:C:2022:601 (Court of Justice of the European Union 2022). https://curia.europa.eu/juris/liste.jsf?language=en&jur=C%2CT%2CF&num=C-184/20&parties=&dates=error&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&alldocrec=alldocrec&docdecision=docdecision&docor=docor&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoor=docnoor&docppoag=docppoag&radtypeord=on&newform=newform&docj=docj&docop=docop&docnoj=docnoj&typeord=ALL&domaine=&mots=&resmax=100&Submit=Rechercher.

[33] 'SS' SIA v Valsts ieņēmumu dienests. (Traitement des données personnelles à des fins fiscales) Request for a preliminary ruling from the Administratīvā apgabaltiesa (Regional Administrative Court, Latvia),, EU:C:2021:690 (Court of Justice of the European Union, Opinion of AG Bobek delivered on 2 September 2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CC0175&qid=1665660436180.

be enough indications to conclude that the names are correctly included in the list, and the data processing requirements must be provided for by law[34]. The Court reached a similar conclusion in *SIA 'SS' v Valsts* case, where it decided that although the collection of taxes and the fight against tax fraud could be considered as tasks in the public interest within the meaning of Article 6(1)(e), a national authority may not derogate from general data protection principles in Article 5(1) GDPR[35].The Court also examined the role of national legislators in developing legal instruments to meet the requirements of Article 6(1)(e) GDPR. In *Latvijas Republikas Saeima* (Penalty Points)[36], the judges found that road safety can meet the **public interest** criterion laid down in Article 6(1)(e), but that further processing activities consisting of making these data available to the wider public (beyond those with a specific interest in the information) and/or to commercial entities for another purpose could not be justified, and that it is up to the Member States to ensure that the legal instruments allowing the processing are themselves in line with the principles of proportionality, necessity and respect for fundamental rights.

The **European Convention on Human Rights** (ECHR) is not a part of the EU legal framework per se, but its significant overlap with the EU Charter and the fact that EU Member States have acceded to the Convention, renders the reference to its provisions, as well as the analysis of its case law, relevant in the context of this study. Unlike the EU Charter, the ECHR does not contain 'third generation' rights such as data protection. However, when considering the processing of personal data for the public interest, Article 8(2) ECHR is particularly relevant, as it provides that a public authority should not interfere with the right to respect for private and family life, '*except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*'. In this Article, the ECHR provides for three key tests enabling States to interfere with the right to respect for private and family life of individuals. The interference must first be in accordance with the law, then it must pursue a legitimate aim, and finally it must be necessary in a democratic society. In its case law, the European Court of Human Rights (ECtHR) identifies both a negative and a positive aspect of the protection of individuals against arbitrary interventions by public authorities (or private bodies to which the State has delegated responsibilities)[37]. The negative aspect of the State's obligation consists of avoiding the violation of the rights of the individual, which includes situations where a private organisation acts as a processor for a public entity[38]. The positive counterpart of this obligation is the duty for States to prevent infringements of individuals' rights by entities, notably through legislation or investigation of breaches. The ECtHR provided guidance for national legislation to comply with the ECHR and regularly found that States failed to meet their obligations under the Convention where their legislation did not provide enough clarity to individuals about their privacy rights[39]. From the Court jurisprudence, it is clear that the States are **expected to implement foreseeable, clear, detailed and publicly accessible**

[34] Peter Puškár v Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy. Request for a preliminary ruling from the Najvyšší súd Slovenskej republiky — Slovakia,, OJ C 402, (Court of Justice of the European Union, Judgment of the Court (Second Chamber) of 27 September 2017 2017).

[35] C-175/20, SIA 'SS' v Valsts ieņēmumu dienests, EU:C:2022:124 (Court of Justice of the European Union (Fifth Chamber) of 24 February 2022). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62020CJ0175.

[36] Proceedings brought by B., Request for a preliminary ruling from Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia),, EU:C:2021:504 (Court of Justice of the European Union, Judgment of the Court (Grand Chamber) of 22 June 2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62019CJ0439&qid=1665649009610.

[37] European Court of Human Rights. (2022). *Guide to the Case-law of the European Court of Human Rights - Data protection*. p. 21.

[38] Vukota-Bojić v. Switzerland, CE:ECHR:2016:1018JUD006183810 (European Court of Human Rights, Judgment (Third Section) of 18 January 2017).

[39] See for instance: Ben Faiza v. France, CE:ECHR:2018:0208JUD003144612 (European Court of Human Rights, Judgment (Fifth Section) of 8 February 2018). , Benedik v Slovenia, CE:ECHR:2018:0424JUD006235714 (European Court of Human Rights, Judgment (Fourth Section) of 24 April 2018). , Rotaru v. Romania, CE:ECHR:2000:0504JUD002834195 (European Court of Human Rights, Jugment (Grand Chamber) of 4 May 2000). , Vukota-Bojić v. Switzerland, CE:ECHR:2016:1018JUD006183810 (European Court of Human Rights, Judgment (Third Section) of 18 January 2017).

legislation in case of an interference with the right to respect for private and family life. The Court's guidance on the application of the ECHR is useful for understanding the GDPR's public interest legal basis requirements and their implementations.

In 2018, **Convention 108+**, amending Convention 108[40] (first binding international instrument on data protection), was adopted and although it is less detailed than the provisions of the GDPR, it represents a key international instrument in this area and is overseen by the Council of Europe. It enables the ECtHR to comment on the wider human rights' implications of data processing, as well as issuing detailed judgements on the Convention.

The **Data Protection Directive 95/46/EC**[41] marked, in the mid-1990s, the first step in the building of the EU legal framework on data protection. It provided for general rules on the legality of personal data processing and data subjects rights and established national DPAs. This framework was significantly reformed in 2016 when the **General Data Protection Regulation** (GDPR)[42] was adopted, repealing the Data Protection Directive 95/46/EC from 2018 onwards, and becoming a key instrument of the EU data protection framework. The GDPR applies to the processing of personal data (data referring to an identified or identifiable natural person[43]) in the scope of EU law, and pursuant to its Article 2 this Regulation only applies where personal data are held in a filing system (manual or electronic), or are intended to be part of such a system[44].

The GDPR provides for a general legal framework for the processing of personal data, and many of its provisions allow Member States to maintain or adopt more specific provisions to further specify them. **Article 6** 'Lawfulness of processing' contains the legal bases under which data may be processed[45]. Some of these legal bases, such as a 'legal obligation' and 'a task carried out in the public interest', must be laid down by Union law or Member State law to which the controller is subject. That legal basis may contain specific provisions adapting certain rules of the GDPR (Article 6(3)). **Article 9** 'Processing of special categories of personal data' imposes a general ban on the processing of special categories of personal data and provides an exhaustive list of grounds or exemptions to lift the ban[46]. Some of these exemptions, such as 'reasons of substantial public interest', must be based on Union or Member State law which also provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

In the context of this study, two legal bases for processing available under Article 6 are particularly relevant to consider and will be analysed in detail in the following Section 5.1 – **Article 6(1)(c)** covering processing necessary to comply with a legal obligation of the controller and **Article 6(1)(e)** allowing processing necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller. Furthermore, **Article 6(3)** specifies that the legal bases for processing referred to in Article 6(1)(c) and (e) shall be provided for either by Union law or by the law of the Member State to which the controller is subject. In order for a legal obligation to fulfil the requirements of a lawful legal basis for processing, in line with Article 6(1)(c), it must at least clearly identify the purpose of the processing, be **proportional** to the legitimate aim pursued and serve a

[40] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), (1981).

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (1995).

[42] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. (GDPR).

[43] Article 4, GDPR.

[44] Article 4, GDPR.

[45] Article 6, GDPR.

[46] Article 9(1) and (2), GDPR.

public interest purpose[47]. Similar requirements are to be met for Article 6(1)(e) to be a valid legal basis. Contrary to Article 6(1)(c), Article 6(1)(e) does not require that the law defines the processing permitted by explicitly determining the purpose of the authorised processing, but rather puts the emphasis on the functions of the body carrying out the processing. Nevertheless, in view of the requirements of **Article 6(3)** to have a legal basis set out by Union or Member State law, and the foreseeability requirements of the EU Charter, it can be concluded that the public interest task or the exercise of official authority vested in the controller must be mentioned in any implementing legislation. Moreover, the purpose of the processing must be necessary for the execution of the task performed in the public interest or in the exercise of official authority vested in the controller.

Recital 45 of the GDPR brings further clarification on Article 6(1)(c) and (e) as it states that where processing is carried out based on these two legal bases, this processing should have a **basis in EU law or Member State law**, which re-emphasises that these provisions require further legislation to legitimise the processing, rather than providing a full and autonomous basis for processing. Such a law may serve as a basis for several individual processing operations, if the official authority of the controller or the public interest is specified for the whole group of processing activities[48]. Recital 45 of the GDPR further states that Union or Member State law should determine the **purpose of the processing**, and may specify the general conditions of the GDPR on several aspects, including the lawfulness of processing, the determination of the controller, the type of personal data that can be processed, the data subjects covered, etc. Furthermore, the recital indicates that EU or Member State law must determine '*whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so* […]'[49]. The recital distinguishes between **public authorities and other entities governed by public law**, without defining the criteria for each category. Thus, although these concepts are put forward in recital 45 with regard to processing in the public interest or in the exercise of official authority, it is left to the EU or Member States to provide such definitions in other legislation.

Regulation (EU) 2021/1057 (ESF+ Regulation) establishes the ESF+, defines its objectives, budget for 2021-2027, the methods of its implementation, the different forms of EU funding and the rules for granting such funding[50]. **Article 17(6)** of the ESF+ Regulation enables Member States to authorise managing authorities and other competent ESF+ bodies to obtain data from registers, provided that this is in line with the legal obligation of the controller' legal basis of Article 6(1)(c) GDPR and public interest legal basis of Article 6(1)(e) GDPR.

Regulation (EU) 2021/1060 (Common Provisions Regulation – CPR 2021)[51], succeeding Regulation 1303/2013 (CPR 2013) covering the previous 2014-2020 programming period, lays down the common provisions to govern eight different funds, including the ESF+. The CPR 2021 and the ESF+ Regulation, define the monitoring and evaluation requirements of the ESF+. In its **Article 4**, the CPR 2021 provides that Member States are allowed to process personal data only if it is necessary to meet their obligations under the CPR 2021 (e.g. for monitoring and evaluation), and in accordance with the GDPR and Regulation (EU)

[47] Article 6(3), GDPR.

[48] Recital 45, GDPR.

[49] Recital 45, GDPR.

[50] Article 1, Regulation (EU) 2021/1057 of the European Parliament and of the Council of 24 June 2021 establishing the European Social Fund Plus (ESF+). .

[51] Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy (CPR).

2018/1725 governing the processing of personal data by the Unions institutions or bodies. Article 4 CPR 2021 and Article 17(6) ESF+ Regulation are thus key in the context of this study, as they allow Member States to use a legal basis to process administrative data for the monitoring and evaluation of the ESF+, in accordance with Article 6 GDPR.

In the European data protection landscape, there are several important actors. First, each Member State has at least one **DPA** responsible for monitoring the implementation of the GDPR, as well as protecting fundamental rights and facilitating the free movement of data. Second, the **European Data Protection Board** (EDPB) is a key body composed of representatives of all national DPAs of the EU Member States and EEA-EFTA countries and a representative of the EPDS. The EDPB is the successor of the WP29 and constitutes an independent body that has been set up to ensure the consistent application of data protection rules throughout the EU, in particular by promoting cooperation between national DPAs and issuing guidance on specific data protection issues. This study will therefore take into account some of these guidelines when analysing the rules applicable to the processing of personal data in relation to the monitoring and evaluation of the ESF/ESF+. Finally, the **European Data Protection Supervisor** (EDPS) is an independent authority established in 2004 responsible for monitoring compliance with Regulation (EU) 2018/1725 by EU institutions and bodies, advising them, intervening before the CJEU as a data protection expert, cooperating with national supervisory authorities and monitoring the potential impact of new technologies on the protection of personal data.

While the GDPR and the national implementing laws apply to EU Member State authorities, **Regulation (EU) 2018/1725** is applicable to EU institutions and bodies when they are processing personal data (with some exceptions concerning certain EU law enforcement agencies and offices when they are processing operational personal data). The content, structure and definitions provided by this Regulation closely follow the approach of the GDPR, in order to have a coherent approach for the protection of personal data in the EU. Regulation (EU) 2018/1725 additionally describes the powers and tasks of the EDPS. Considering that the Regulation applies to the processing of personal data by EU institutions and bodies[52], and does not apply to national authorities, it places it largely outside the scope of this study.

Regulation (EC) 1338/2008 lays down a common framework for the systematic production of EU statistics on public health and health and safety at work[53]. Article 7 on transmission, treatment and dissemination of data provides that, when Member States have to transmit confidential data necessary for the production of EU statistics, they should make sure that the data subjects are not identifiable and that the personal data are protected in compliance with EU data protection rules. Thus, this Regulation does not have implications for the monitoring and evaluation of the ESF+ and is therefore outside the scope of this study.

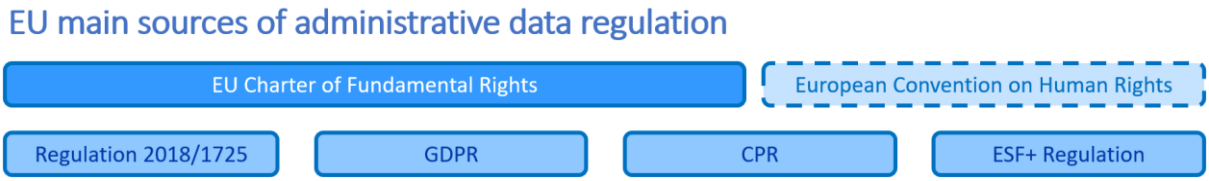
Furthermore, **Regulations (EU) 2021/1056, 2021/1058 and 2021/1059** are also outside the scope of this research, as they respectively establish the Just Transition Fund, set out the objectives and scope of support of the European Regional Development Fund, and lay down the rules of the European territorial cooperation goal.

The main legal sources described above are presented in Figure 2.

[52] Article 2, Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[53] Article 1, Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work.

Figure 2: EU main sources of administrative data regulation



Box 3: Key findings – EU level legal framework

- The European legal framework is composed of several elements:
- EU primary legislation contains provisions on data protection, such as Article 16(1) of the TFEU, Article 8 of the EU Charter, as well as rights connected to data protection, such as the right to respect for private and family life (Article 7 EU Charter). Article 52 also provides for a balancing test for interfering with fundamental rights, including the right to data protection.
- The case law of the CJEU gives guidance on the processing of data based on Article 6(1)(c) and (e), on the legal obligation of the controller and public interest.
- The GDPR, successor to the Data Protection Directive, is the key instrument of the EU data protection acquis. Article 6 lists the legal bases for processing data, including the necessary processing to comply with a legal obligation of the controller (Article 6(1)(c)) and the performance of a task carried out in the public interest (Article 6(1)(e)). Article 6(3) requires the processing to have a legal basis in Union or Member State law, which emphasises the need for further legislation to legitimise the processing. Article 9 GDPR imposes a general ban on processing special categories of personal data, with an exhaustive list of exceptions.
- The ESF+ Regulation through its Article 17(6), and the CPR 2021 with its Article 4, allow Member States to process personal data if in accordance with the GDPR and Regulation 2018/1725.
- Several actors are important in the European data protection landscape, including the DPAs of each Member States, to monitor GDPR implementation and protect rights, the EDPB, ensuring the consistent application of data protection rules throughout the EU, the EDPS, monitoring compliance with Regulation 2018/1725 by EU institutions and bodies.

4.2. Outline description of national legal frameworks

This Section aims to describe the overarching national legislative framework for data protection in nine selected Member States: Austria, France, Germany, Ireland, Italy, Poland, Romania, Spain and Sweden. For each of these countries, this Section identifies the GDPR-implementing laws, the national legislation complementing the CPR 2021 and the ESF+ Regulations, the existing Partnership Agreements, the national Courts having jurisdiction over data protection matters, and the national DPAs. In relation to the competent Courts, it is interesting to highlight that national DPA's decisions are usually of an administrative nature, and data subjects can have recourse to a judicial review against these decisions, in accordance with Article 78 GDPR. It is thus for national courts to decide on the interpretation

of GDPR provisions and national GDPR-implementing laws.

Austria

The primary legislative instrument implementing the GDPR in Austria is the **Federal Act concerning the Protection of Personal Data** (*Bundesgesetz über den Schutz personenbezogener Daten – Datenschutzgesetz* – DSG)[54]. This law does not strictly follow the structure of the GDPR but rather incorporates the GDPR provisions into national law and reserves the discretion granted to Member States only for two instances: cases of emergencies, and cases of '*processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*'[55]. The DSG also makes a reference to Article 8 of the ECHR by requiring all laws adopted in accordance with the DSG to use the least intrusive measures necessary to achieve the stated objectives, to incorporate safeguards for the protection of the rights of individuals, as well as include the notion of 'necessity' in line with Article 8(2) of the ECHR[56].

The *Datenschutzbeuftragter* (DSB) is the **Austrian DPA**. This body, inter alia, checks that legislation contains sufficient detail to comply with the requirements of the law when assessing future processing activities[57]. The competent court to hear data protection cases in Austria is the **regional court** (*Landsgericht*).

Austria implemented the Operational Programme Employment in line with the ESF Regulation in the 2014-2020 period[58]. For the next period, Austria provided itself with the **ESF+ Programme Employment Austria & JTF 2021-2027**[59]. The latter instrument does not contain specifications relating to data processing applicable to the monitoring and evaluation of the ESF+. This is also the case for the Special Directive of the Federal Minister for Work, Social Affairs and Consumers protection on the implementation of projects in the framework of the European Social Fund 2014-2020[60].

France

The main instrument for implementing the GDPR in France is the **Law on information technology, files and freedoms** (*Loi relative à l'informatique, aux fichiers et aux libertés* - LIL)[61], later amended by Law n° 2018-493 of 20 June 2018 relating to the protection of personal data[62]. It directly incorporates or refers to large parts of the GDPR, while also using

[54] Federal Act concerning the Protection of Personal Data (DSG) (Bundesgesetz über den Schutz personenbezogener Daten) (Austria). https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html

[55] Part 2, 'Data processing for specific purposes', DSG.

[56] Article 1, DSG.

[57] Decision DSB-D213.1020, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 16 August 2020). https://www.dsb.gv.at/download-links/dokumente.html.

[58] Operational programmes within the Framework of the objective "Investment for Growth and Employment" - Austria (Operationelle Programme im Rahmen des Ziels "Investitionen in Wachstum und Beschäftigung"), (2014).

[59] ESF+ Programme Employment Austria & JTF 2021-2027 - Austria (ESF+ Programm Beschäftigung Österreich & JTF 2021-2027), (2021).

[60] Special Directive of the Federal Minister for Work, Social Affairs and Consumers protection on the implementation of projects in the framework of the European Social Fund (ESF) 2014-2020 - Austria (Sonder-Richtlinie des Bundesministers fuer Arbeit, Soziales, und Konsumentenschutz zur Umsetzung von Projekten im Rahmen des Europaeischen Sozialfonds (ESF) 2014-2020), (2019).

[61] Law on Information Technology, Data Files and Civil Liberties (Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/ (LIL).

[62] Law relating to the protection of personal data, amending Loi n°78-17 du 6 janvier 1978 (Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952.

Member State's discretion in a number of important areas. The LIL stresses that a legal basis to process special categories of personal data under Article 9 GDPR is enough to make the operation lawful, without needing an additional legal basis under Article 6 GDPR[63].

The **French DPA** is the *Commission Nationale de l'Informatique et des Libertés* (CNIL). The body has a broad mandate and several mandatory responsibilities, including approving various government measures concerning personal data. The French GDPR implementing law, in contrast to other implementing laws in other Member States, gives legislative powers to the CNIL by requiring it to adopt rules to regulate certain areas of processing. It thus diverges from the role of a regulating or approval body, and enables the CNIL to become a source of the legal basis for certain processing operations. The decisions from the CNIL can be appealed to the **State Council** (*Conseil d'Etat*).

No **ESF+ implementing law** was found for France. The Decree n°2016-126 of 8 February 2016 on the implementation of programmes co-financed by the European structural and investment funds for the period 2014-2020 does not provide any information on data protection matters[64].

Germany

The key **GDPR-implementing law** at the federal level in Germany is the **Federal Data Protection Act** (*Bundesdatenschutzgesetz* – BDSG)[65]. It implements many areas left to national discretion in the GDPR and bases its structure on the distinction between the processing of personal data by private and public sector bodies. This national legislation provides a clear indication of which data can be processed by public entities, how data can be transmitted to public and private bodies and how they can reuse the data. Section 3 of the BDSG states that '*Public bodies shall be permitted to process personal data if such processing is necessary to perform the task for which the controller is responsible or to exercise official authority which has been vested in the controller*'.

The **German DPA** is the *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI) and is responsible for advising the German federal government, parliament, Bundesrat, and other bodies on legislative and administrative issues relating to the protection of personal data[66]. Moreover, each of the 16 German federal states (*Länder*) also has a DPA, which is competent for monitoring and enforcing the GDPR, including any data protection legislation at the level of a particular federal state. Bavaria is an exception as it has two DPAs, one competent for monitoring and enforcing the GDPR, including any data protection legislation specifying or restricting the GDPR at the state level for private (non-public) bodies in Bavaria; and one overseeing data protection legislation for public bodies. Decisions from the BfDI can be appealed to the **local district court** or the **regional court**. Cases involving up to EUR 100 000 in monetary fines are dealt with by the local district court and the regional court deals with cases involving higher sums.

No relevant element for data protection was found in the **ESF Plus Federal programme for 2021-2027**[67]. The document laying down the funding principles for the authorisation of Grants from the ESF+ in the Funding period 2021-2027 provides that for '*the 2021-2027*

[63] Article 4(5), LIL.

[64] Decree n°2016-126 of 8 February 2016 on the implementation of programmes co-financed by the European structural and investment funds for the period 2014-2020 - France (Décret n°2016-126 du 8 février 2016 relatif à la mise en œuvre des programmes cofinancés par les fonds européens structurels et d'investissement pour la période 2014-2020), (2016). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032000333.

[65] Federal Data Protection Act (Bundesdatenschutzgesetz). (BDSG).

[66] Article 14(3), BDSG.

[67] Programmes ESF Plus 2021-2027 Bund - Germany (ESF Plus Programm 2021 - 2027 Bund).

funding period, predetermined participant characteristics, results of the funding, as well as other project-related material data (e.g. indicators) will be collected and stored electronically.'[68] It is specified that the obligation stems from Article 17 ESF+ Regulation, and that the aggregate material data for the projects are transmitted to the EU twice per year by managing authorities in the Federal Ministry of Labour and Social Affairs. The document additionally states that material data must be collected at project level regularly and continuously and recorded electronically, in compliance with data protection law.

Ireland

In Ireland, the primary legislative instrument implementing the GDPR is the **Data Protection Act 2018**[69]. Its structure is quite similar to that of the GDPR and uses much of the language of the EU Regulation. It is interesting to note that the Irish implementation of the legal basis for processing in the public interest (Article 6(1)(e) GDPR) specifies that the term 'official authority' encompasses non-statutory public schemes, programme or funds, and requires a particular legislative procedure to legitimise the processing[70]. This procedure entails that, prior to passing legislation legitimising particular processing activities, Ministers must consult all concerned relevant stakeholders (including the Irish DPA). For processing special categories of personal data for reasons of substantial public interest, the Data Protection Act requires a special regulation authorising such processing which should identify, not just the substantial interest concerned, but also the suitable and specific measures to be taken to safeguard the fundamental rights and freedoms of data subjects in processing the authorised personal data. Similarly, as in the case of processing in public interest, the Minister must consult the Irish DPA[71]. Additionally, the Data Sharing and Governance Act 2019[72] can also be useful, as it provides a list of entities considered to be public bodies[73] and lays down some of the requirements for a public body to share data with another public body[74].

The **Data Protection Commission** is the Irish DPA and is responsible for safeguarding the right to data protection through the enforcement and evaluation of the application of Irish data protection legislation. The scope of this body's powers, functions and duties are laid down in the Data Protection Act 2018. Decisions issued by the Irish Data Protection Commission can be appealed to the **Circuit court** (for fines below EUR 75 000), or to the **Irish High Court**.

Circular 13/2015 Management and control procedures for the European Structural and Investment Funds Programmes 2014-2020[75] does not contain any relevant provision on data protection. The same applies to Circular 08/2015 National Eligibility Rules for Expenditure Co-Financed by the European Regional Development Fund (ERDF) Under Ireland's Partnership Agreement 2014-2020[76].

[68] Funding principles for the authorisation of Grants from the ESF Plus in the Funding period 2021-2027 - Germany (Fördergrundsätze für die Bewilligung von Zuwendungen aus dem ESF Plus in der Förderperiode 2021-2027), (2022).

[69] Data Protection Act 2018 (Ireland). https://revisedacts.lawreform.ie/eli/2018/act/7/revised/en/html

[70] Section 38, Data Protection Act (Ireland) 2018.

[71] Section 51, Data Protection Act (Ireland) 2018.

[72] Data Sharing and Governance Act 2019 (Ireland).

[73] Section 10, Data Sharing and Governance Act 2019 (Ireland).

[74] Section 13, Part 3, Data Sharing and Governance Act 2019 (Ireland).

[75] Circular 13/2015 Management and control procedures for the European Structural and Investment Funds Programmes 2014-2020 (Ireland).

[76] Circular 08/2015 National Eligibility Rules For Expenditure Co-Financed By The European Regional Development Fund (ERDF) Under Ireland's Partnership Agreement 2014-2020 (Ireland).

Italy

The main GDPR-implementing legislative instrument in Italy is the Legislative Decree of June 2003, no.196, **Code regarding the protection of personal data** (*Decreto legislative 30 giugno 2003, n.196 Codice in materia di protezione dei dati personali*)[77]. Most of its sections have specific requirements regarding the legislation legitimising the processing, which often involves the approval of the Italian DPA, and a public consultation (e.g., it is the case for processing in the public interest[78]).

Italy's DPA is the ***Garante***. It has some semi-legislative powers from the Italian Data Protection Code, although they were reduced following an amendment to the Code[79]. It has the power to scrutinise legislation adopted by the Italian government to ensure its compliance with data protection law and the rules adopted by the Italian DPA constitute the national legal basis for most of the processing activities. Data subjects in Italy may bring complaints to the Garante and directly to the **ordinary courts**.

No ESF+ implementation law was found for Italy during the research for this study.

Poland

The most significant legal instrument in Polish national law related to the GDPR is the **Act of 10 May 2018 on the Protection of Personal Data** (*Ustawa z 10 maja 2018 o ochronie danych osobowych* - APPD)[80]. This Act largely follows the GDPR text and structure, but the legislation itself mainly legislates to implement the discretion granted to Member States in some areas to restrict the data subjects' rights in certain situations. For instance, the scope of Articles 13 to 15 GDPR (Information to be provided and right of access by the data subject) are restricted to situations where the processing is performed on the basis of public interest[81]. However, for cases in which rights are restricted, safeguards must be established.

The Polish DPA is the **Personal Data Protection Office** (UODO), and its competences are set out in the Polish Data Protection Law (APPD). The body, inter alia, conducts and issues administrative decisions, conducts audits of compliance and provides guidelines and opinions. In the context of the COVID-19 pandemic, the President of the UODO re-emphasised the need for specific legislative instruments to enable data processing[82]. The **National Administrative Court** and the **Regional Administrative Court** are both competent to review decisions from the UODO.

Act of 11 July 2014 concerning rules of implementation of programmes supported from Cohesion Policy in the financial period 2014-2020 mentions that '*Data on project*

[77] Legislative Decree No 196 of 30 June 2003 - Personal Data Protection Code, containing provisions for the adaptation of the national system to Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC. (Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679) (Italy). https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig (Italian Data Protection Code).

[78] Chapter II, Article 2 et seq., Italian Data Protection Code.

[79] Decree-law No. 139 of 8 October 2021 (Decreto-legge 8 ottobre 2021, n. 139) (Italy). https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2021-12-07&atto.codiceRedazionale=21A07259&elenco30giorni=true.

[80] Act of 10 May 2018 on the Protection of Personal Data (Ustawa z 10 maja 2018 o ochronie danych osobowych). https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000 (APPD).

[81] Articles 3 to 5a, APPD.

[82] Opinion of the President of the Office on the draft regulation of the Minister of Family, Labour and Social Policy amending the regulation on social welfare homes to the problem of the functioning of the COVID-19 outbreak, 04 September 2020. https://uodo.gov.pl/pl/file/3752 p.118.

participants within the meaning of Annex I or II of the ESF Regulation collected in the central data communication system may be made available to the President of the Social Insurance Institution in connection with in relation to the implementation of tasks resulting from Art. 50 section 3a and 3c of the Act of 13 October 1998 on the social insurance system (Journal of Laws of 2020, item 266, 321 and 568).'[83]. Chapter 18 of **Act of 28 April 2022** on the rules for the implementation of cohesion policy programmes financed in the financial perspective 2021-2027[84] specifically deals with processing of personal data and access to registers. Furthermore, the Guidelines on the conditions of collection and transmission of data in electronic form for the period 2014-2020[85] provides measures to ensure uniform rules for the utilisation of the Central Information System inter alia for monitoring and evaluation and determine the minimum scope and form of information to be supplied using this system in the implementation of cohesion policy programmes.

Romania

The key GDPR implementing legislation in Romania is **Law no. 190/2018** on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)[86]. This implementing law is primarily designed to implement Article 6(2) and Article 9(4) GDPR. The legal bases for data processing under Law no. 190/2018 are largely based on the text of the GDPR as reflected in Article 6 of the implementing law, dealing with the processing of personal data and special categories of personal data for tasks carried out in the public interest[87]. The different sections of Law no.190/2018 refer to the GDPR as well as further safeguards to be established according to the type of processing envisaged. For instance, Article 6 of Law no.190/2018 envisages additional legislation in order to legitimise specific data processing activities.

The Romanian DPA is the **National Supervisory Authority for the Processing of Personal Data** (ANSPDCP) and is responsible for monitoring and controlling the lawfulness and legitimacy of processing personal data activities falling under Romanian law. Sanctions imposed by the ANSPDCP can be appealed by **ordinary courts** of the place of residence of the plaintiff or the court of domiciliation of the defendant (in the case of the ANSPDCP, the Bucharest tribunal).

No national ESF+ implementing law was found for Romania during the research for this study.

[83] Article 71, Act of 11 July 2014 concerning rules of implementation of programmes supported from Cohesion Policy in the financial period 2021-2027 (Ustawa z dnia 11 lipca 2014 o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020) (Poland).

[84] Act of 28 April 2022 on the rules for the implementation of cohesion policy programmes financed in the financial perspective 2021-2027 (Ustawa z dnia 28 kwietnia 2022 o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2021-2027) (Poland).

[85] Guidelines on the conditions of collection and transmission of data in electronic form for the period 2014-2020 (Wytyczne w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020) (Poland).

[86] Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Romania).

[87] Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Romania).

Spain

The **Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights** (*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*)[88] is Spain's main GDPR-implementing legislation. This legislation directly implements many provisions of the GDPR, requiring in the majority of cases that any domestic legislation legitimising the processing of personal data must have the status of law in Spain[89].

The Spanish DPA is the ***Agencia Espanola Proteccion Datos*** (AEPD) and is responsible for guaranteeing privacy and data protection to individuals in Spain. It has several functions, including consultative ones (to the Parliament, Public administrations, citizens, data protection officers), as well as advisory, informative and awareness-raising functions. Decisions from the AEDP can be appealed to the **National Court** (Administrative Litigation Division) and to the **Third Chamber of the Supreme Court** for an appeal of the first instance decision.

In addition to the AEPD, there are also three **autonomous regional data protection agencies** created by regional laws: the Council for Transparency and Data Protection of Andalusia, the Basque Data Protection Agency and the Catalan Data Protection Authority. For decisions of these agencies, the court having jurisdiction is the Supreme Court of Justice of the Autonomous Community.

No relevant **ESF+-implementing measures** were found for Spain in the context of this study. The Resolution of 22 December 2021, of the Secretary of State for Social Rights, publishing the Agreement of the Territorial Council of Social Services and the System for Autonomy and Care for Dependency, on the programming of the ESF+, in relation to the objective of combating material deprivation, does not provide any provisions on data protection[90].

Sweden

The **Data Protection Act** is Sweden's GDPR implementing law, and contains supplementary provisions to the EU data protection regulation (*SFS 2018:218 Lag med kompletterande bestämmelser till EU:s dataskyddsförordning*)[91]. The legislation complements the provisions of the GDPR but does not significantly expand on them. Chapter II of the Swedish Data Protection Act lays down the bases for processing data and largely reproduces the text of the GDPR. Concerning the type of legal instrument required to process data, the implementing law includes all the possible options set out in the GDPR[92]. Furthermore, according to Chapter 3 Section 3 of the Data Protection Act, the processing of sensitive personal data by a public authority, on the basis of Article 9(2)(g)

[88] Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales). (Spain).

[89] See for example, Articles 8(1) and (2) and Article 9(2) of the Organic Law 3/2018 (Spain).

[90] Resolution of 22 December 2021, of the Secretary of State for Social Rights, publishing the Agreement of the Territorial Council of Social Services and the System for Autonomy and Care for Dependency, on the programming of the European Social Fund Plus, in relation to the objective of combating material deprivation (Resolución de 22 de diciembre de 2021, de la Secretaría de Estado de Derechos Sociales, por la que se publica el Acuerdo del Consejo Territorial de Servicios Sociales y del Sistema para la Autonomía y Atención a la Dependencia, sobre la programación del Fondo Social Europeo Plus, en relación con el objetivo de lucha contra la privación material) (Spain).

[91] Act (2018:218) containing provisions supplementing the EU Data Protection Regulation (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning) (Sweden). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218

[92] See for example: Chapter 2 Section 1 (Legal obligation), Section 2 (Task carried out in the public interest) and Chapter 3 Section 3 (Substantial public interest for sensitive personal data).

GDPR may be possible if the data have been provided to the authority and the process is required by law; if the processing is necessary for the purpose of the processing of a case; or if the processing is necessary for an important public interest and does not constitute an unwarranted intrusion into the personal integrity of the data subject.

The Swedish DPA is the **Authority for Privacy Protection** (IMY) and is responsible for the protection of individuals' personal data and privacy in particular by ensuring that the data protection legislation is complied with. It seeks to safeguard the fundamental data protection rights of individuals and to facilitate the free movement of these data. IMY decisions may be appealed to the **General Administrative Court**.

The Act (2007:459) on structural fund partnerships[93], the Ordinance (2014:1374) on the management of the Fund for European Aid to the Most Deprived[94], the Ordinance (2007:907) containing instructions for the Swedish ESF Council[95] and the Swedish ESF Council regulations and general advice on ESF support under the national social fund programme[96], are the most relevant legislations when it comes to the ESF implementation in Sweden. However, none of them contain provisions on data protection.

Box 4: Key findings – National legal framework

This Section has described the national legal framework for data protection for the nine selected Member States, to have an overall context for the following Sections.

- The main legislative instrument implementing the GDPR in Austria is the Federal Act concerning the Protection of Personal Data (DSG), the *Datenschutzbeuftragter* (DSB) is the Austrian DPA and the competent court to hear data protection cases is the regional court. The ESF+ Programme Employment Austria & JFT 2021-2027 covers the ESF+ period but does not contain specifications relating to data processing applicable to the monitoring and evaluation of the ESF+.

- The main instrument for implementing the GDPR in France is the LIL, CNIL is the French DPA, whose decisions can be appealed to the State Council. No ESF+ implementing law was found for France.

- The main legislative instrument implementing the GDPR in Germany is the Federal Data Protection Act (BDSG), the BfDI is the German DPA and additionally, each of the 16 German federal States has a DPA. The decisions of BfDI can be appealed to the local district court or regional court. The document laying down the funding principles for the authorisation of grants from the ESF+

[93] Act (2007:459) on Structural Funds Partnerships (Lag (2007:459) om strukturfondspartnerskap) (Sweden), (2007). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007459-om-strukturfondspartnerskap_sfs-2007-459.

[94] Ordinance (2014:1374) on the management of the Fund for European Aid to the Most Deprived (Förordning (2014:1374) om förvaltning av fonden för europeiskt bistånd till dem som har det sämst ställt) (Sweden), (2014). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20141374-om-forvaltning-av-fonden_sfs-2014-1374.

[95] Ordinance (2007:907) containing instructions for the Swedish ESF Council (Förordning (2007:907) med instruktion för Rådet för Europeiska socialfonden i Sverige) (Sweden), (2007). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2007907-med-instruktion-for-radet_sfs-2007-907#:~:text=Chefen%20f%C3%B6r%20enheten%20beslutar%20i,besluta%20om%20en%20s%C3%A5dan%20delegering.

[96] Swedish ESF Council regulations and general advice on ESF support under the national social fund programme (Svenska ESF-rådets föreskrifter och allmänna råd om stöd från Europeiska socialfonden inom ramen för det nationella socialfondsprogrammet).

in the 2021-2027 funding period provides some elements regarding the transmission of aggregate material data.

- The main legislative instrument implementing the GDPR in Ireland is the Data Protection Act 2018, the Data Protection Commission is the Irish DPA and the decisions and fines issued by the latter can be appealed to the Circuit court or to the Irish High Court. No relevant information was found in documents related to the implementation of the ESF/ESF+.

- The main legislative instrument implementing the GDPR in Italy is the Legislative Decree of June 2003, no.196, Code regarding the protection of personal data, and the Garante is the Italian DPA, whose decisions can be appealed directly to the ordinary courts. No ESF+ implementation law was found for Italy.

- The main national legislative instrument supplementing the GDPR in Poland is the Act of 10 May 2018 on the Protection of Personal Data (APPD) and the UODO is the Polish DPA, whose decisions can be reviewed by the National Administrative Court and the Regional Administrative Court. Act of 11 July 2014 concerning rules of implementation of programmes supported from Cohesion Policy in the financial period 2014-2020, Act of 28 April 2022 on the rules for the implementation of cohesion policy programmes financed in the financial perspective 2021-2027 and the Guidelines on the conditions of collection and transmission of data in electronic form for the period 2014-2020 provide useful elements on the processing and transmission of personal data.

- The main legislative instrument implementing the GDPR in Romania is Law no. 190/2018, and the ANSPDCP is the Romanian DPA, whose decisions can be appealed by ordinary courts. No national ESF/ESF+ implementing law was found for Romania.

- The main legislative instrument implementing the GDPR in Spain is the Organic Law 3/2018, of 5 December 2018, on Personal Data Protection and guarantee of digital rights, and the Agencia Espanola Proteccion Datos (AEPD) is the Spanish DPA, whose decisions can be appealed to the National Court and to the Third Chamber of the Supreme Court. Additionally, there are three autonomous regional data protection agencies for Andalusia, the Basque Country and Catalonia, whose decisions can be reviewed by the Supreme Court of Justice of the Autonomous Community. No relevant ESF+-implementing measures were found for Spain.

- The main legislative instrument implementing the GDPR in Sweden is the Data Protection Act and the IMY is the Swedish DPA, whose decisions may be appealed to the General Administrative Court. The Swedish legislation regarding ESF/ESF+ does not contain data protection provisions.

4.3. Examples of dataset and sectoral-specific legislation

As demonstrated in the description of the EU legal framework above, several pieces of legislation need to be taken into account to understand how personal data is to be processed in the Member States. The EU Charter and the ECHR must be respected, and any processing activity must additionally be in line with the provisions of the GDPR, the CPR 2021, the ESF+ Regulation, and Regulation 2018/1725, when applicable. In addition, national legislation must also be observed, and here again, several levels of instruments

must be considered. The processing of personal data must comply with the requirements of the national constitutions, the national GDPR implementation laws, the national sectoral and dataset-specific laws, as well as with the sector-specific data soft-law.

While general rules are provided in overarching legal instruments such as the GDPR, these do not always provide detailed rules on how to deal with each specific type of data and thus often allow Member States to adapt these rules or provide for more specific rules - in specific sectors. This Section builds on the previous ones and focuses on the national regimes of Austria, Romania and Spain. Administrative datasets, such as the ones used for the ESF monitoring and evaluation belong to the public sector and are therefore governed by public law of each Member States. In order to better grasp the different legislation that may need to be taken into account in the reuse of administrative data for the monitoring and evaluation of the ESF/ESF+, three examples of sector-specific laws are considered. Through examples of how social security data in Austria, tax data in Romania and data from surveys in Spain are regulated, one can understand the multiplicity of national rules applicable to each public sector data.

Austria

The study's focus chosen in Austria to better grasp the different legislations that might be involved in the processing of personal data of each sector is **social security data**. The main Austrian GDPR-implementing law to consider is the **Federal Act concerning the Protection of Personal Data** (DSG)[97]. It is therefore the first instrument to be considered when examining the rules applicable to the reuse of social security database in Austria.

Section I of the **Federal law on the social insurance institution for the self-employed**[98] (Self-Employed Social Security Act) provides for rules regarding the obligation of information and clarification, as well as the electronic data processing. Paragraph 9 in particular states that '*The insurance carrier is authorised to process personal data insofar as this is an essential requirement for the fulfilment of the tasks assigned to it by law. The tasks assigned to him by law also include the transmission of the data necessary for the collection of the cost contributions provided for in Section 27a of the Federal Act on Hospitals and Health Resorts*'[99].

Furthermore, the **Labour Market Service Act**[100] is also useful to consider as it provides for rules on confidentiality in its Section 27, and Section 25 covering data protection and states that '*the Public Employment Service, the Federal Administrative Court and the Federal Ministry of Labour, Social Affairs, Health and Consumer Protection are authorized to process personal data within the meaning of the Data Protection Act, Federal Law Gazette I No. 165/1999 insofar as this is an essential prerequisite for the fulfilment of their statutory tasks*'[101].

Additionally, depending on the exact type of data to be reused, other legislative instruments might need to be taken into account, such as the **Unemployment Insurance Act**[102], the

[97] Federal Act concerning the Protection of Personal Data (DSG) (Bundesgesetz über den Schutz personenbezogener Daten) (Austria). https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html.

[98] Federal law on the social insurance institution for the self-employed (Self-Employed Social Insurance Act) (Selbständigen-Sozialversicherungsgesetz) (Austria), (2018).

[99] Paragraph 9, Self-Employed Social Security Act (Austria).

[100] Labour Market Service Act (Arbeitsmarktservicegesetz) (Austria).

[101] Section 25, Labour Market Service Act.

[102] Unemployment Insurance Act (Arbeitslosenversicherungsgesetz) (Austria).

Collective Labour Relations Act[103], or the **Social Insurance Organisation Act**[104]. Section 30 of the latter instrument for instance deals with umbrella associations of social security institutions, and Section 30(d)(2) in particular provides that '*The umbrella organisation is obliged to adopt a data protection regulation for all social security institutions and to publish it on the Internet*'[105].

Romania

An overview of the legislation applicable to the **reuse of tax data in Romania** is useful to have an insight into the different national rules that may be applicable to such processing activities in a specific sector.

First, the main national legislation supplementing the GDPR in Romania is **Law no. 190/2018** on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC[106]. The implementation law, however, does not provide specifications related to the processing of tax data and thus needs complementing sectoral legislation.

The **Fiscal Procedure Code**[107] provides useful information on the nature of data collected and its storage. Article 59(4) states that: '*[…] in order to clarify and establish the real tax situation of taxpayers, the specialised departments of local public administration authorities shall have the power to request information and documents of tax relevance or for the identification of taxpayers or taxable or taxable matter, as appropriate, and notaries public, lawyers, bailiffs, police, customs, Community public services for driving licences and vehicle registration, Community public services for issuing simple passports, Community public services for personal records, and any other entity holding information or documents relating to taxable or taxable goods, as the case may be, or to persons who are taxpayers, shall be obliged to provide them free of charge*"[108]. Additionally, **Law No. 571** of 22 December 2003, regarding the Fiscal Code[109] contains some information on the electronic database regarding intra-Community operations in its Article 158[110].

The **Decision No 23/2012**[111] issued by the national DPA describes the cases where it is not necessary to notify the data subject regarding the processing of personal data. The Decision establishes that no notification of processing personal data is necessary in cases where this processing is carried out by a public administration authority at local or national level in order to fulfil their legal duties[112]. Government Decision No 520 of 24 July 2013 on the

[103] Collective Labour Relations Act (Austria).

[104] Social Insurance Organisation Act (Sozialversicherungs-Organisationsgesetz) (Austria).

[105] Section 30(d)(2), Social Insurance Organisation Act (Austria).

[106] Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Romania).

[107] Fiscal Procedure Code (Codul de Procedură Fiscală) (Romania). https://lege5.ro/Gratuit/g4ztkmrygm/codul-de-procedura-fiscala-din-2015.

[108] Article 59(4), Code of Fiscal Procedure (Codul de Procedură Fiscală) (Romania).

[109] Law No. 571 of December 22, 2003 regarding the Fiscal Code (Romania).

[110] Article 158, Law No. 571 (Romania).

[111] Decision No 23/2012 regarding the establishment of cases in which it is not necessary to notify the processing of personal data (Decizia Nr.23 din 26.03.2012 privind stabilirea cazurilor în care nu este necesară notificarea prelucrării unor date cu caracter personal) (Romania). http://www.legex.ro/Decizia-23-2012-119333.aspx.

[112] Article 1(e), Decision No 23/2012 (Romania).

organisation and functioning of the National Tax Administration Agency[113] may be useful when the reuse of tax data involves the National Tax Administration Agency.

Spain

The example chosen for Spain to illustrate the multiplicity of legislation to be taken into account in each single sector is the **reuse of telephone numbers by a public authority for the purpose of carrying out surveys**.

The first national legislative instrument to be taken into account is the **Spanish GDPR-implementing law**, the Organic Law 3/2018, of 5 December on Personal Data Protection and guarantee of digital rights (LOPDGDD)[114]. Article 11 dealing with transparency and information to the affected party[115], and Article 26 on the processing of data for archiving purposes in the public interest by public administration are particularly relevant in this context[116].

Additionally, several other laws are to be considered for the processing of telephone numbers for another public purpose. **Law 9/2014**, of 9 May, General Telecommunications[117] regulates telecommunications in general, and its Chapter III in particular deals with the confidentiality of communications and the protection of personal data, as well as public rights and obligations in relation to electronic communications networks and services. **Law 12/1989**, of 9 May, on the Government Statistics Act covers public statistical functions for the purposes of the central government[118], and provides particularly useful information its Chapter II on data collection. **Law 39/1995**, of 19 December, on the Organisation of the Sociological Research Centre[119] can also be interesting to consider, as its Article 5 exposes the principles of action and the legal regime applicable to the survey research, including voluntary responses and personal data protection[120]. Furthermore, **Law 39/2015**, of 1 October, on the Common Administrative Procedure of Public Administrations[121] covers, inter alia, the administrative procedures common to all public administrations and must therefore be considered in case of transmission of personal data from one public authority to another for another purpose.

Moreover, regulatory rules must be taken into account as well. In particular, Title V of the **Royal Decree 424/2005** of 15 April 2005 approving the Regulation on the conditions for the provision of electronic communications services, universal service and the protection of users, is to be considered, as it covers the obligations of a public nature related to the secret

[113] Government Decision No 520 of 24 July 2013 on the organisation and functioning of the National Tax Administration Agency (Hotărârea Guvernului Nr. 520 din 24 iulie 2013 privind organizarea şi funcționarea Agenției Naționale de Administrare Fiscală) (Romania).

[114] Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).

[115] Article 11, LOPDGDD.

[116] Article 26, LOPDGDD.

[117] Law 9/2014, of 9 May, General Telecommunications (Ley 9/2014, de 9 de mayo, General de Telecomunicaciones) (Spain).

[118] Law 12/1989, of 9 May, on the Government Statistics Act (Ley 12/1989, de 9 de mayo, de la Función Estadística Pública) (Spain).

[119] Law 39/1995, of December 19, on the Organization of the Sociological Research Center (Ley 39/1995, de 19 de diciembre, de Organización del Centro de Investigaciones Sociológicas) (Spain).

[120] Article 5, Law 39/1995 (Spain).

[121] Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas) (Spain).

of communications and personal data protection[122]. The **Order CTE/711/2002** of 26 March 2002 laying down the conditions for providing the telephone consultation service on subscriber numbers[123] and the **Circular of the National Commission on Markets and Competition 1/2013**[124] on the procedure for the provision of subscriber data for the provision of directory services, telephone consultation on subscriber numbers and emergencies, as amended by Circular 5/2014 of 30 July 2014 are also to be considered in this context.

Finally, the Spanish DPA (AEPD) published several reports dealing with the possible transmission of telephone numbers for another purpose[125], and on the communication of phone numbers between public authorities[126], that can be used in the assessment of the lawfulness of such data processing operations.

Box 5: Key findings – Examples of dataset and sectoral-specific legislation

This Section focused on examples of sector-specific laws for the national regimes of Austria, Romania and Spain. It gave an overview of the different pieces of legislation to be considered when dealing with social security data in Austria, tax data in Romania or survey data in Spain. These three examples of in-depth analyses provide an insight into the diversity and multiplicity of national legislation to be taken into account for each different public sector data. They are meant to illustrate that answers to data protection dilemmas and questions in case of monitoring and evaluation of ESF/ESF+ programmes are not straightforward and cannot be explained solely through interpretation of EU data protection rules. In order to comply with the legal requirements in accessing administrative data for monitoring and evaluation purposes, one should study not just national GDPR implementing laws and ESF/ESF+ implementing laws but also (pre-) existing national sectoral laws and database specific laws, depending on the sector and type of data. For this reason, the approach adopted in the following Sections, which analyse the data protection aspects relevant to the monitoring and evaluation of ESF+, focuses solely on the EU level legislation and the general national data protection framework.

[122] Title V, Royal Decree 424/2005 of 15 April 2005 approving the Regulation on the conditions for the provision of electronic communications services, universal service and the protection of users (Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios) (Spain).

[123] Order CTE/711/2002, of 26 March, laying down the conditions for the provision of the telephone enquiry service on subscriber numbers (Orden CTE/711/2002, de 26 de marzo, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado) (Spain).

[124] Resolution of 20 March 2013, of the Telecommunications Market Commission, publishing Circular 1/2013, regarding the procedure for the provision of subscriber data for the provision of directory services, telephone enquiries about subscriber numbers and emergencies (Resolución de 20 de marzo de 2013, de la Comisión del Mercado de las Telecomunicaciones, por la que se publica la Circular 1/2013, relativa al procedimiento de suministro de datos de los abonados para la prestación de servicios de guías, consulta telefónica sobre números de abonado y emergencias) (Spain).

[125] Report 31/2020, of 7 April, on the possible transfer to the CIS, by the National Statistics Institute (INE), of the landline and mobile telephones of the population selected in the samples to carry out the functions attributed to the CIS (Informe 31/2020, de 7 de abril relativo a la posible cesión al CIS, por parte del Instituto Nacional de Estadística (INE) de los teléfonos fijos y móviles de la población seleccionada en las muestras para ejecutar las funciones atribuidas al CIS) (Spain).

[126] Report 35/2020 of 27 April, concerning the communication by the CNMC to the CIS of the fixed and mobile telephones of the selected and mobile telephones of the population selected in the nominative samples which are prepared for the CIS by the INE (Informe 35/2020, de 27 de abril, relativo a la comunicación por la CNMC al CIS de los teléfonos fijos y móviles de la población seleccionada en las muestras nominativas que son elaboradas para el CIS por el INE) (Spain).

5. Analysis of the data protection aspects relevant to the monitoring and evaluation of the ESF+

Data collected by public authorities (i.e., administrative data), which are used for ESF/ESF+ monitoring and evaluation include personal data. The purpose of this Section is hence to analyse the data protection aspects relevant to the monitoring and evaluation of the ESF/ESF+ at the EU level and in the three Member States (Austria, Romania, and Spain) selected for the in-depth review as listed in Task 2 of the Technical Specifications[127]. The analysis is based on desk research, which focused on the EU and national data protection legal framework applicable to the current ESF+ programming period and was supplemented with the jurisprudence of the CJEU and the ECtHR as well as national case law and any relevant guidelines, opinions, and decisions of the national DPAs. Whilst results of the stakeholder interviews and the legal analysis will be brought together for the purpose of the Final Report, this Section already provides some illustrative examples from interviews especially in the three Member States. These examples in the form of Boxes aim to further substantiate the legal analysis. The illustrative examples should, however, be read with a certain degree of caution as the interview findings mostly relate to practices applicable to the previous ESF programming period, while the legal analysis focuses on the existing ESF+ programming period.

Section 5.1 provides an analysis of the most appropriate legal basis for the processing of personal data in the context of monitoring and evaluation of the ESF+. Section 5.2 focuses on the reuse of data and also discusses the reuse of data for scientific research purposes. Consent as a special legal basis is dealt with in Section 5.3, while Section 5.4 analyses the possibility to process special categories of personal data. Sections 5.5 and 5.6 deal with data transmission and data linking, respectively. Section 5.7 looks at the legal obligations regarding storing data for evaluations and monitoring. Finally, Section 5.8 analyses the conditions and practical implications of the requirement to inform data subjects about the processing of their data.

5.1. Legal basis for the monitoring and evaluation of the ESF+

This Section provides analysis on the legal basis for the monitoring and evaluations of the ESF+. After a general discussion on the possible legal basis provided in the GDPR and in the national GDPR-implementing laws in a selected number of Member States (Sub-section 5.1.1), the report explains provisions on the legal basis in specific EU and national laws that regulate the ESF+ monitoring and evaluations (Sub-section 5.1.2).

5.1.1. Possible legal bases for processing administrative data for the ESF+ monitoring or evaluation

The requirement to have a legal basis is a prerequisite for any processing operation and mirrors the data protection principle of lawfulness[128]. The GDPR requires that any entity (private or public) or an individual processing personal data to which the GDPR applies

[127] Technical Specifications, pp. 9-13.

[128] Principle of lawfulness is one of the basic principles relating to the processing of personal data and the request that data are processed lawfully, meaning that the controller must be able to demonstrate a lawful legal basis for obtaining personal data to be processed. See Article 5(1)(a), GDPR.

must do so based on a valid legal basis, as set out in the text of the GDPR or in Member State's law in an area of national discretion contained in the GDPR. This Sub-section hence analyses possible legal bases that could be used by entities processing data for the ESF+ both in case of monitoring (e.g., processing of participants data) or evaluation (e.g., processing of participants and non-participants data).

Possible legal bases for processing of personal data under Article 6 GDPR are:

(a) data subject's consent;
(b) processing is necessary for the preparation or performance of a contract to which the data subject is a party;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary to protect the vital interests of the data subject or another person;
(e) processing is necessary for the performance of a task in the public interest or the exercise of official authority vested in the controller; and
(f) processing is necessary for the legitimate interests of the controller, provided those interests do not override the rights of the data subject.

It is important to note that the list of possible legal bases in GDPR is **exhaustive** (closed list), meaning that for processing to be lawful, personal data should be processed on one or more legal bases as provided for in Article 6(1) GDPR. While national GDPR implementation laws or other laws can further specify some of the legal bases (in particular in case of legal obligation and public interest legal bases), they cannot go beyond the rules set out in the GDPR and create other or different legal bases.

Where **special categories of personal data (sensitive data)** are processed, all general principles and rules of the GDPR apply as well, including the condition for lawful processing. Additionally, Article 9 GDPR provides an exhaustive list of grounds or exemptions under which the processing of special categories of personal data is allowed despite the general prohibition for such processing. Issues connected with the processing of special categories of personal data for the purposes of monitoring and evaluation of the ESF/ESF+ are discussed in detail in Section 5.4 below.

Based on the principle of accountability[129], it is the obligation of the controller to be able to demonstrate compliance with data protection principles, including the lawfulness of processing. As controllers are the ones who determine the purposes and means of the processing of personal data[130], they have the responsibility to also ensure that there is an appropriate legal basis for every processing operation. The ability to rely on legal bases mentioned in Article 6(1) GDPR does not exempt the controller from complying with the other requirements of the GDPR and potential national GDPR-implementing laws[131].

There are in principle several legal bases which could, under certain conditions, be applicable to the processing of personal data for the ESF/ESF+ monitoring or evaluation. However, as visible from the analysis below, **the most appropriate legal bases for processing personal data for ESF/ESF+ monitoring or evaluation – both in case of processing participants data and non-participants data - are compliance with a legal obligation (letter (c)) and performance of a task carried out in the public interest (letter (e)), which necessitate the processing**. As explained in Sub-section 5.1.2, these

[129] Article 5(2), GDPR.

[130] Article 4(7), GDPR.

[131] European Data Protection Board. (2019a). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0*. p. 4.

legal bases are also chosen as the most appropriate legal bases when accessing data from national administrative registers for the current ESF+ programming period 2021-2027[132].

Stakeholder interviews showed that during the previous ESF programming period of 2014-2020, consent was in particular used in case of collection of personal data from participants[133]. It remains to be seen, if the fact that the EU legal framework now explicitly mandates Member States to enable certain processing operations through national law, will result in the shift in national practices. To this end, stakeholders in Ireland and Sweden are already asking to use legal bases other than consent.

Box 6: Examples from the stakeholder interviews – Legal basis

In Ireland, the data protection advisors of the intermediary bodies suggested that legal basis to collect data should not be based on consent but rather on the legal obligation or on (significant) public interest to process data. In Sweden for example, challenges regarding the burden to collect (explicit) consent from ESF participants were overcome by relying on the 'legal obligation' legal basis under Article 6(1)(c) GDPR. To this end, the Swedish Public Employment Service, who acts as a beneficiary as well as an administrative authority, made an internal legal assessment and concluded that several national provisions, when read jointly, could be interpreted as to oblige them to collect and share data for the realisation of ESF/ESF+ projects.

The legal basis of **legitimate interests** in Article 6(1)(f) GDPR is out of reach for public authorities when they are performing their tasks[134]. Hence, it cannot be used to justify processing of data for ESF/ESF+ monitoring or evaluation purposes. This legal basis can be used if processing is necessary to achieve the legitimate interests of a controller or a third party (e.g., such interests can include commercial interests, individual interests, or broader societal benefits), unless there are overriding interests or fundamental rights and freedoms of data subjects, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller[135]. As a result, this legal basis entails an extra responsibility for controllers as they need to perform a balancing test against the interests or fundamental rights and freedoms of the data subject and inform the data subject about it. Since public authorities cannot rely on legitimate interests when processing (e.g., collecting, linking or sharing) personal data in performance of their tasks, this legal basis is not further elaborated. The notion of 'public authority' is not defined in the GDPR, allowing the EU and Member States' legislations to determine the scope of this term. One could argue that since the Audit Authorities of each Member State must be public authorities according to Article 71(2) CPR 2021 and since managing authorities must be established

[132] Article 17(6), ESF+ Regulation. Note that the EU legislation under the previous programming period did not include such a clear choice of the legal basis.

[133] See in particular Sub-section 3.1.1, which explains that only in Sweden consent is not systematically collected to process participants' personal data.

[134] Article 6(1) last sentence GDPR clearly states that legitimate interests cannot apply to processing carried out by public authorities in the performance of their tasks. This legal basis is hence reserved for private law controllers or for public authorities if they are processing data for a legitimate reason other than performing their tasks as a public authority. Please note that under the Data Protection Directive legitimate interests could be relied upon by public and private sector. See for example Article 29, Data Protection Working Party. (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 26.

[135] See in particular recital 47, GDPR.

by each Member State[136], it is likely that the European courts (CJEU or ECtHR) would consider them as public authorities also for the purposes of GDPR and ECHR[137].

Similarly unsuitable are legal bases of a **contract** with a data subject (Article 6(1)(b) GDPR) and **vital interests** (Article 6(1)(d) GDPR). With respect to the former, Article 6(1)(b) GDPR provides a lawful basis to the extent that "processing is necessary for the performance of a **contract** to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract"[138]. For this legal basis to apply, either of the two conditions should be met: (i) the processing in question must be objectively necessary for the performance of an existing contract **between a controller and a data subject**; or (ii) the processing must be objectively necessary in order to take pre-contractual steps at the request of a data subject[139]. Considering the nature of the relationship between participants of ESF/ESF+ programmes and the ESF/ESF+ managing authorities, it is not possible to claim that the processing of individuals' personal data is happening from the necessity to perform contractual obligations towards data subjects or to enter into a contract with them. In case of processing of non-participants' data, it is conceptually impossible to use this legal basis to any data processing for counterfactual impact evaluations, as the individuals whose data will be used for this evaluation do not have an opportunity to contract with any ESF/ESF+ authorities. Moreover, in its Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects[140], the EDPB held that a contract must be a legally enforceable contract, under the national contract law, for this legal basis to apply. The controllers hence need to demonstrate that (i) a contract exists, (ii) such a contract is valid pursuant to applicable national contract laws, and (iii) that the processing is objectively necessary for the performance of the contract. As for the legal basis of **vital interests** of the data subject or another person, recital 46 GDPR makes it clear that this legal basis should be interpreted narrowly and only used where the processing cannot manifestly be based upon another legal basis. This legal basis is thus reserved for situations where the life of an individual is in danger, not enabling him or her to provide consent for the processing. National-level research in the three Member States selected for in-depth analysis (Austria, Romania, and Spain) confirms the EU-level analysis.

Consent, which is a valid legal basis specified in Article 6(1)(a) GDPR, is discussed in more detail in Section 5.3 below, including the question on whether a controller could migrate from consent to another legal basis.

This Section looks more specifically at two of the most appropriate legal bases for processing data for the ESF/ESF+ monitoring and evaluation – compliance with a **legal obligation** (Article 6(1)(c) GDPR) and performance of a task carried out in the **public interest** (Article 6(1)(e)).There are some clear similarities between Article 6(1)(c) and Article 6(1)(e), as both legal bases must be based on EU or Member State law. However, while public interest legal basis is restricted to the public sector, nothing limits the application of legal obligation to the private or public sector. As mentioned by the CJEU, the nature and

[136] Article 71(2), Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy (CPR).

[137] For example, the ECtHR has commented on the nature of 'public authorities' in cases *Costello-Roberts v. the United Kingdom,, CE:ECHR:1993:0325JUD001313487 (European Court of Human Rights, Judgment (Chamber) of 25 March 1993). , The Holy Monasteries v. Greece, nos. 13092/87 and 13984/88 (European Court of Human Rights, Judgment (Chamber) of 9 December 1994).* In the latter, the Court stated that: "*the State cannot absolve itself from responsibility [under the ECHR] by delegating its obligations to private bodies or individuals*".

[138] See also recital 44, GDPR.

[139] European Data Protection Board. (2019a). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0*. p. 8.

[140] Ibid.

the purpose of processing should be considered at the outset, meaning that determining a lawful legal basis should be the first task an entity should consider[141].

Firstly, the compliance with a **legal obligation** is discussed.

Article 6 (1)(c) GDPR provides that:

> *"1. Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> *[…]*
>
> *(c) processing is **necessary** for compliance with a **legal obligation** to which the controller is subject;"*
>
> *GDPR, Article 6(1)(c)*

In addition to Article 6(1)(c), Article 6(3) specifies that:

> "3. *The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:*
>
> *(a) Union law; or*
>
> *(b) Member State law to which the controller is subject.*
>
> ***The purpose of the processing shall be determined in that legal basis** or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall **meet an objective of public interest** and be **proportionate to the legitimate aim** pursued."*
>
> *GDPR, Article 6(3)*

Moreover, Article 6(2) gives Member States additional discretion stating that:

> "*2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX."*

Further clarification on the requirements for the legal obligation may be found in recital 41, which provides that:

[141] X and Z v Autoriteit Persoonsgegevens. Request for a preliminary ruling from the Rechtbank Midden-Nederland (District Court, Central Netherlands, Netherlands),, EU:C:2021:822 (Court of Justice of the European Union, Opinion of AG Bobek delivered on 6 October 2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CC0245&qid=1665650857775.

> *"Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be* ***clear and precise*** *and its application should be* ***foreseeable to persons*** *subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights."*
>
> *GDPR, recital 41*

In addition, recital 45 also clarifies the legal basis in Articles 6(1)(c).

Taking together all elements and additional requirements of Article 6, for a legal obligation to be a valid legal basis under Article 6(1)(c), it must

- originate directly from EU or Member State law;
- be sufficiently clear, precise and foreseeable;
- determine the purposes of the processing;
- be proportionate to the legitimate aim pursued;
- be for an objective of public interest.

The scope of legal obligation as a legal basis is thus strictly delimited. Although such legal obligation must be imposed by law making the obligation valid and binding, it is not necessary that a legal obligation is laid down in a legislative act, adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned[142]. Moreover, the legislation may in some cases set only a general objective, while more specific obligations are imposed at a different level (e.g. in secondary or sectorial legislation or by binding decisions of public authorities)[143].

The element that the law should be proportionate to the legitimate aim pursued requires (national) legislators to perform a clear balancing of rights to privacy and data protection in accordance with Article 8(2) ECHR and Articles 7 and 8 of the EU Charter. Case law of the ECtHR and the CJEU provides further guidance on this. Difficulties could arise if legal instruments are lawful - and enforceable in a certain Member State but would not meet the requirements set out in the GDPR. In such cases, controllers (and also processors) would be bound by a legal obligation requiring them to perform certain data processing procedures. However, the legal obligation itself would not meet the requirements for reliance on Article 6(1)(c) GDPR to legitimise that processing.

Secondly, the compliance with the performance of a task carried out in the **public interest** is discussed.

Article 6 (1)(e) GDPR provides that:

> *"1. Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> *[…]*

[142] Recital 41, GDPR. Note that a contractual obligation, voluntary unilateral engagements and public-private partnerships cannot be seen as a valid legal basis. See also Data Protection Working Party. (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. pp. 19-20.

[143] Ibid.p. 20.

> *(e) processing is **necessary** for the performance of a task carried out in the **public interest** or in the **exercise of official authority** vested in the controller;"*
>
> *GDPR, Article 6(1)(e)*

Also, for this legal basis, provisions in Article 6(2) and (3) provide further requirements and give Member States' laws additional discretion.

In addition, recital 45 clarifies Articles 6(1)(e), including that:

> *"[…] This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. […]"*
>
> and
>
> *"[…] It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association."*
>
> *GDPR, recital 45*

For controllers to be able to rely on the legal basis under Article 6(1)(e), the following conditions must be fulfilled:

- originate from EU or Member State law;
- indication of a task in a public interest or official authority vested in the controller;
- the purpose of the processing needs to be necessary for the performance of a task or the exercise of official authority;
- must be proportionate to the legitimate aim pursued.

In contrast to Article 6(1)(c), for Article 6(1)(e) there is no requirement that the legal basis shall determine the processing permitted by explicitly defining the purpose of processing. However, in light of the requirements under Article 6(3) for the legal basis to be laid down by Union or Member State law read together with recital 45, it should be noted that the processing must, however, be linked to and be necessary for the performance of a specific task carried out in the public interest or in the exercise of official authority vested in the controller. WP29 Opinion from 2014 suggests that, since legitimate interests in Article 6(1)(f) is excluded as a legal basis for public authorities from the GDPR, public interest in Article 6(1)(e)) should be interpreted in such a way as to allow public authorities some degree of flexibility[144].

The text of the GDPR does not specify whether the official authority must be vested in a public sector body, leaving this matter to Member States' discretion[145]. As explained above, **the notion of 'public authority'** is not defined in the GDPR. The same is true for the **notion**

[144] Ibid.p. 23.

[145] Recital 45, GDPR.

of 'public interest', allowing national legislators to determine the scope of these terms in relation to specific processing activities. Following analysis of the CJEU and the ECtHR case law as well as of academic literature on these concepts, it proved to be impossible to provide a uniform definition. Very few national GDPR-implementing laws of the nine Member States provide clear definitions, meaning that the terms public authority and public interests would need to be interpreted based on the provisions of their entire legal systems and traditions[146].

Similarly, to Article 6(1)(c), Article 6(1)(e) requires **EU or national legislators to consider the fundamental rights or interest of data subjects** when passing legal instruments that require processing in the public interest to be carried out, as both of these legal bases entail a **necessity test** (i.e. the processing should pass the proportionality and subsidiarity test).

As explained in Section 4.1, case law of the CJEU and the ECtHR provide further guidance on the application of these legal bases. The CJEU appears to consider that the Member State must ensure that legal instruments enabling processing are themselves in accordance with the principles of necessity, proportionality and respect for fundamental rights.

Equally important is the case law of the ECtHR, as rights conferred by the ECHR are also contemplated by the GDPR, most significantly the right to respect for private and family life in Article 8[147]. The ECHR contains three key tests for a state to interfere with the Article 8 rights of an individual, found in Article 8(2). The interference must be: 'in accordance with the law', must pursue a 'legitimate aim' and must be 'necessary in a democratic society'. The ECtHR has provided guidance on the requirements for national legislation to be in accordance with the ECHR and has regularly found states to be in breach of their obligations where laws have failed to provide sufficient clarity for individuals in relation to their rights relative to the respect for privacy[148]. In the case *Marper v UK*[149] the ECtHR stated that the law must be sufficiently clear to give individuals an understanding of the circumstances in which public authorities are empowered to use mass surveillance. The Court noted that the law must indicate the extent of any discretion public authorities may enjoy and must provide sufficient detail in the description of how such discretion is to be exercised, so that individuals may be able to challenge any arbitrary interference[150]. In a more recent case, the Court stressed that storing excessive amounts of data could not be permissible simply on the basis that a greater quantity of data increased the effectiveness of the system[151]. In addition to the CJEU case law, the jurisprudence of the ECtHR seems to request that Member States need to implement clear, sufficiently detailed and foreseeable legislation to justify any interference with Article 8 ECHR rights, and that such legislation should be

[146] For example, Article 66 of the French LIL, which regulates processing of health data in the public interest, creates a regulatory framework to determine the type of entity who may act as a controller. Under this Section, private entities could be included but would need to have a special authorisation by the national SA. On contrary, in Austria, Section 10 DSG creates a specific regulatory mechanism to determine bodies who are permitted to process data for public interest such as public sector entities and "relief organisation". Moreover, Section 26 DSG intends to draw a distinction between public-sector and private sector controllers.

[147] Most notably in its language of "necessity" and "proportionality"; see European Commission. *Why do we need the Charter?* Retrieved 12 October 2022 from https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en#:~:text=The%20Charter%20strengthens%20the%20protection,and%20freedoms%20in%20the%20Charter.

[148] See in particular: Ben Faiza v. France, CE:ECHR:2018:0208JUD003144612 (European Court of Human Rights, Judgment (Fifth Section) of 8 February 2018). , Vukota-Bojić v. Switzerland, CE:ECHR:2016:1018JUD006183810 (European Court of Human Rights, Judgment (Third Section) of 18 January 2017). Paragraphs 58-61; Benedik v Slovenia, CE:ECHR:2018:0424JUD006235714 (European Court of Human Rights, Judgment (Fourth Section) of 24 April 2018). , Rotaru v. Romania, CE:ECHR:2000:0504JUD002834195 (European Court of Human Rights, Jugment (Grand Chamber) of 4 May 2000).

[149] S. and Marper v. the United Kingdom,, CE:ECHR:2008:1204JUD003056204 (European Court of Human Rights, Judgment (Grand Chamber) of 4 December 2008). Paragraphs 99, 103.

[150] In another case, the Court requested the publication of subsidiary regulations or guidelines. See Shimovolos v. Russia,, CE:ECHR:2011:0621JUD003019409 (European Court of Human Rights, Judgment (First Section) of 21 June 2011).

[151] Gaughran v. the United Kingdom,, CE:ECHR:2020:0213JUD004524515 (European Court of Human Rights, Judgment (First Section) of 13 February 2020).

publicly accessible. Larger interference with rights should consequently attract more detailed and clearer legislation, with more stringent safeguards to protect personal data.

Finally, legal bases in Article 6(1)(c) and (e) enable **further discretion by Member State law** in a sense that such national laws may contain specific provisions to adapt the application of the GDPR rules, as stated in Article 6(3) GDPR. This refers to all material law of a Member State but not of a third country outside the EU/EEA legal area. Therefore, legal obligations enshrined in third country regulations or tasks carried out in the public interest of a third country or in the exercise of official authority vested by virtue of a foreign law, fall outside the scope of these two legal bases[152].

By way of comparison, the following Table 12 shows which of the three Member States selected for the in-depth legal analysis have chosen to legislate in the areas of their discretion.

Table 12: Matrix of three Member States decisions to exercise discretion in case of key legal bases

Member State	Article 6(1)(c) – legal obligation	Article 6(1)(e) – public interest
Austria	No	No
Romania	No	Yes
Spain	Yes	Yes

A specific legal basis can only be relied upon if existing legislation or new legislation that is passed meets the criteria required for such a law in the GDPR. This does not necessarily have to be a data protection law and could also be any other existing (sectorial) law[153].

In the case of **Austria**, Section 4(1) DSG makes the GDPR applicable to the processing of personal data, unless there are more specific provisions. As such, legal bases in Article 6 GDPR are not further elaborated in Austrian data protection law. Moreover, the DSG contains a transitional provision that preserves the legal provisions relating to personal data of pre-existing laws[154]. As a result, both post- and pre-GDPR legislation could in principle be considered to provide a lawful basis for processing as far as it contains provision(s) providing for a legal obligation or a task carried out in the public interest which necessitate the processing of personal data. In the opinion of the Austrian Constitutional Court, the legislation allowing public authorities to interfere with data protection rights must describe with sufficient precision the conditions under which it is permissible to identify or use the data for the performance of specific administrative tasks and the extent and nature of the administrative discretion[155].

[152] See for example Data Protection Working Party. (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 21. Although this opinion was based on the text of the old Data Protection Directive, it could still be used as the text of the GDPR in Article 6(1)(c) and (e) largely reflects the wording in the old Directive.

[153] For illustration of this please see Section 0 above.

[154] Section 69(8), DSG.

[155] Decision of the Constitutional Court, 15 June 2007, VfSlg. 18.146/2007. https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vfgh&Sammlungsnummer=18146&SkipToDocumentPage=True&Suche

In contrast, **Spain** exercised its discretion both in the case of Article 6(1)(c) as well as Article 6(1)(e). Spain's GDPR-implementing law (Organic Law 3/2018) provides that a legal obligation should be written in a norm with a **force of law** and may determine the general conditions of the processing, the types of data, as well as the transfers that may take place as a consequence of compliance with the legal obligation. Moreover, such a legal provision may lay down appropriate measures in line with Chapter IV GDPR[156]. In Spain, processing based on public interest legal basis is also only lawful if the task carried out in the public interest, or the exercise of official authority vested in the controller, derives from a competence conferred by a regulation having the force of a law[157]. Hence, a legal basis needed in Spanish law for situations under Article 6(1)(c) and (e) must be established in primary legislation that cannot give the public body discretion to decide on the scope of its public interest task[158].

Romanian GDPR-implementing law (Law no. 190/2018) claims to mainly implement Article 6(2) and 9(4). Article 6 of Law no. 190/2018 regulates processing for the performance of a task in the public interest and provides safeguards to be established by the controller or the third party, such as appropriate technical and organisational measures, designating a data protection office and establishing retention periods. As such this Article requires additional national legislation to legitimise a specific processing operation.

The examples above show that to conclude on a legal basis under Article 6(1)(c) or (e), one needs to look further than the national data protection laws.

5.1.2. Provisions on the legal basis in EU and national laws for processing administrative data for ESF+ monitoring or evaluation

The following legal provisions relevant for personal data processing applicable to the current ESF+ programming period have been identified.

While the CPR 2013 applicable to the past ESF programming period did not touch upon the issue of processing personal data, **Article 4 CPR 2021** stipulates that **Member States are allowed to process personal data** in order to meet their obligations under the CPR 2021 (including for monitoring and evaluation of the ESF+), and such processing has to be **in accordance with the GDPR**:

> *The Member States and the Commission shall be allowed to process personal data only where necessary for the purpose of carrying out their respective obligations under this Regulation, in particular for monitoring, reporting, communication, publication, evaluation, financial management, verifications and audits and, where applicable, for determining the eligibility of participants. The personal data shall be processed in accordance with Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 of the European Parliament and of the Council (40), whichever is applicable.*
>
> *CPR 2021, Article 4*

NachRechtssatz=False&SucheNachText=True&ResultFunctionToken=e9c97a3e-8d9d-4e7a-a34e-429b1611f4be&Dokumentnummer=JFT_09929385_06G00147_00.

[156] Article 8(1), Organic Law 3/2018.

[157] Article 8(2), Organic Law 3/2018.

[158] Judgment 292/2000 of 30 November 2000, BOE [Official Gazette] number 4, of 04 January 2001 (Constitutional Court). https://hj.tribunalconstitucional.es/HJ/en/Resolucion/Show/4276.

Article 44(4) CPR 2021 further requires from the Member States or the managing authorities to ensure that the **necessary procedures** are set up to produce and collect the data necessary for evaluations. Several other provisions in the CPR 2021 are also of relevance for the processing of data. For example, in order to fight fraud of expenditure, Member States must, in line with Article 69(2) CPR 2021, process information on beneficial owners of the recipients of Union funding. Such processing must be done **in line with the applicable data protection rules**. Article 69(4) CPR 2021 further states that it is also on the Member States to **ensure accuracy and reliability of the monitoring system** and of data on indicators. CPR 2021 also provides rules on national authorities. To this end Article 72(1)(e) states that the managing authorities should record and store electronically the data on each operation necessary for monitoring and evaluation and ensure the security, integrity and confidentiality of data and the authentication of users, whereas Article 82 provides for a retention period (e.g. a 5-year period from 31 December of the year in which the last payment by the managing authority to the beneficiary is made). Reference to compliance with privacy and data protection is also done in Article 2.5. of Annex XV, whilst Article 2.6. of the same Annex talks about the obligation of Member States to adopt information security policies. Finally, Article 42(1) CPR 2021 on the transmission of data explains that the ESF+ Regulation may determine specific rules for the frequency of collecting and transmitting longer-term result indicators.

With respect to **ESF+ Regulation**, **recital 33** makes it clear that the processing of personal data within the framework of the ESF+ Regulation should be **in line with the GDPR**, that the dignity of and respect for the privacy of end recipients of operations should be guaranteed and that in order to avoid any stigmatisation, the persons receiving food and/or basic material assistance should not be required to identify themselves when receiving the support and when taking part in surveys on the most deprived persons who have benefitted from the ESF+[159].

Based on **Article 17(1) ESF+ Regulation**, all programmes benefitting from general support from the ESF+ strand under shared management shall use common output (measuring the actions taken in a project, such as training a certain number of people) and results indicators (measuring the immediate effect of the project on participants, such as finding employment within a few months of the project) to monitor progress implementation. Those common indicators which are set out in Annex I could include participants' data and result in the processing of personal data[160].

Article 17(6) of the ESF+ Regulation provides a rule on processing data in national administrative registers and explains that:

> *Where data are available in registers or equivalent sources, Member States **may enable** the managing authorities and other bodies entrusted with data collection necessary for the monitoring and the evaluation of general support from the ESF+ strand under shared management **to obtain data from those registers or equivalent sources, in accordance with Article 6(1), points (c) and (e), of Regulation (EU) 2016/679**.*
>
> *ESF+ Regulation, Article 17(6)*

Article 17(6) of the ESF+ Regulation stipulates that **Member States could grant access to personal data in administrative registers based on Article 6(1)(c) or (e) GDPR**. It is important to note that whilst Article 4 CPR 2021 provides a general provision for any processing within the framework of ESF+ monitoring or evaluations, Article 17(6) ESF+ Regulation is limited to situations where managing authorities or other national bodies need

[159] This recital goes further than the recital 16 of the ESF Regulation that only instructed Member States to take into account data protection requirements linked to processing of participants special categories of personal data, without mentioning compliance with other GDPR rules and principles.

[160] E.g., Article 17(3) ESF+ Regulation requires that the reported values of the output indication are expressed in absolute numbers.

to obtain data from administrative sources and not directly from individuals.

The importance of clear and specific national provisions is stressed by national DPAs and courts. Whilst Austrian and Spanish DPAs and courts did not (yet) provide any specific guidance regarding the processing of data for ESF+ monitoring and evaluations, the Romanian DPA - ANSPDCP provided such advice.

Box 7: Example from the stakeholder interviews – Advice from the Romanian DPA

The National Unemployment Agency for instance requested an opinion from the Romanian DPA (ANSPDCP) on processing information related to education in the context of ESF. Regarding the possibility of concluding a protocol with the Ministry of Education for communicating such data to the Unemployment Agency, the ANSPDCP replied that the Romanian legislation must be aligned to the requirements imposed under the GDPR and thus need to create a legal basis (for instance a legal obligation) for such transmission of data. The ANSPDCP held that a protocol alone cannot constitute a legal basis for data processing and that the legal basis should be provided by law.

In addition, the **Romanian DPA** also commented on the nature of the legal obligation legitimising the processing of data (Article 6(1)(c)) in comparable situations. In its opinion regarding digital social vouchers[161], the ANSPDCP, citing the CJEU case of *Bara v Romania*[162], argued that the requirement for legislative transparency (foreseeability) meant that the instrument setting out the nature of processing should be **a 'regulatory administrative act' rather than a 'protocol' without the force of a published legal instrument**[163]. The ANSPDCP took a similar position when asked to comment on the draft legislation enabling parents to take time from work to supervise children during the pandemic[164] and on the draft legislation allowing teaching to be conducted online during the pandemic[165]. It emphasised that legislation must be specific in its description of the processing activities; for example, the terms 'electronic transmission' and 'through technology and the internet' were seen as too broad and general. On the contrary, when considering the lawfulness of employers monitoring employees during remote working, the ANSPDCP found that national legislation provided sufficient legal basis for such

[161] This Opinion discussed the draft emergency law that intends to provide digital social vouchers for hot meals to people over 75 years of age whose income is at the level of social allowance and to the homeless.

[162] Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF),, OJ C 381 (Court of Justice of the European Union, Judgment of the Court (Third Chamber) of 1 October 2015 2015). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CA0201&qid=1665651259899.

[163] Opinion on Emergency Ordinance (OUG) 115/2020, which provides for the issuing of digital social vouchers of 180 lei per month for hot meals to people over 75 years of age whose income is at the level of social allowance and to the homeless, with the necessary amounts to be provided from non-reimbursable external funds, 07 April 2021, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro.

[164] Review of draft Government Emergency Ordinance on granting free days to parents for the supervision of children, in the event of the suspension of courses or the temporary closure of some educational establishments due to the spread of the coronavirus SARS — COV-2. (Gov Emergency Ordinance 147/2020), 24 September 2020, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro.

[165] Review of draft Government Emergency Ordinance on taking measures for the proper functioning of the education system and amending and supplementing the National Education Law no. 1/2011, 29 July 2020, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro.

processing[166]. The opinion stressed that the national law provides that further conditions for this processing should be laid down in the individual employment contract, the employer's internal regulations and/or applicable collective agreement(s). Additionally, an employer that monitors its employees needs to respect the principles of data minimisation and proportionality and document such internal processing procedures, including the balancing test explaining that employer's legitimate interests outweigh the interests of data subjects (employees). With respect to the legal basis under Article 6(1)(e) the Romanian High Court of Cassation and Justice Judgement held that the authorisation for the Competition Authority to 'obtain data' was sufficient to cover inspection of telephones, and 'other limits' on data collection were not required to be mentioned[167]. In another case against the Tax Authority, the Court found that legislation enabling tax authorities to collect data is sufficient to comply with data protection law[168].

Although the Austrian and Spanish DPA did not provide any specific advice related to the processing of data for ESF, their general guidance and opinions on the topic of processing (administrative) data by public authorities is important. **In Austria**, for example, the DPA provided guidance to public authorities processing data under national implementing legislation[169]. In a decision on the job-seeker support app 'AMS-Algorithmus', designed to predict the outcome of jobseeker training and interventions, the Austrian DPA found that the use of the app exceeded the legal basis provided by the national Labour Market Services Act (AMSG)[170]. This was because the recent COVID-19 pandemic had resulted in fewer face-to-face consultations with jobseeker specialists and as such the predictions of the algorithm were 'unquestioned.' Acknowledging that not every single activity of a public authority can be exhaustively cited by law, the Austrian DPA essentially said that public authorities may process personal data if legislation defines clear conditions for interference with the fundamental right to data protection. As such, the DPA found that the app had exceeded the legal basis for its use of data and required more detailed legal provisions to allow the algorithm to make 'automated decisions' about jobseekers[171]. Although this decision was later annulled by the Federal Administrative Court[172], it still demonstrates that **a greater interference with the fundamental right to data protection, requires a greater level of detail in the determination of the corresponding legal basis** (so called risk-based approach)[173]. The Austrian DPA stressed the importance of clear and specific national legal provisions also at several other occasions[174]. In its 2020 *Opinion on Draft Federal Act amending the 1950 Epidemic Act, the Tuberculosis Act and the COVID-19 Measures Act*, the DPA for instance said that at a minimum, the Act should include examples of the categories of data that could be processed[175]. Furthermore, in the decision

[166] Opinion on Employee Data Processing in the Context of Telework Activity, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro.

[167] Decision no. 2804 of 12 May 2021, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

[168] Decision no. 2216 of 02 June 2020, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

[169] Decision DSB-D213.1020, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 16 August 2020). https://www.dsb.gv.at/download-links/dokumente.html.

[170] Ibid.

[171] Ibid., p. 3.

[172] Decision of the Federal Administrative Court, 18 December 2020, W256 2235360-1/5E. https://gdprhub.eu/index.php?title=BVwG_-_W256_2235360-1.

[173] Decision DSB-D213.1020, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 16 August 2020). https://www.dsb.gv.at/download-links/dokumente.html.

[174] See for example Data Protection Implications of Contact Tracing Apps, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 16 August 2020). https://www.dsb.gv.at/download-links/dokumente.html.

[175] Opinion Opinion on Draft Federal Act amending the 1950 Epidemic Act, the Tuberculosis Act and the COVID-19 Measures Act, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 16 August 2020 2020). https://www.parlament.gv.at/PAKT/BEST/SN/index.shtml, pp. 1-2.

on the Vienna Contact Tracing Regulations[176], the Austrian DPA held that the Vienna Regulations, in combination with the amended Epidemic Act, did not provide a sufficient legal basis for the mandatory collection of health data for contact tracing because together "*they did not reveal clear or precise rules on the scope of the interference with the fundamental right to data protection and therefore did not comply with the requirement of transparency within the meaning of Article 5(1)(a) of the GDPR*"[177].

Box 8: Key findings – Legal basis

- Any kind of processing of personal data, including processing of participants' data for ESF/ESF+ monitoring purposes and processing of participants and non-participants' data for ESF/ESF+ evaluation purposes, needs to be lawful, meaning that it needs to have a legal basis.
- Legal analysis shows that although several legal bases in Article 6 GDPR could be used to legitimise the processing of participants and non-participants personal data for the ESF/ESF+ monitoring or evaluation, the most appropriate legal bases seem to be (i) compliance with a legal obligation (Article 6(1)(c)) and (ii) performance of a task carried out in the public interest (Article 6(1)(e)).
- Article 6(1)(c) and (e) GDPR require EU or Member States to establish the legal bases under these provisions by law and leave some discretion on certain aspects of data processing, as defined in Article 6(2) and (3) GDPR. Review of national GDPR-implementing laws shows that two out of three Member States selected for an in-depth analysis used this option (Romania only for letter (e) and Spain both for letters (c) and (e)).
- Article 17(6) of the ESF+ Regulation stipulates that Member States may enable relevant authorities to process personal data from national administrative registers in accordance with the GDPR legal basis concerning processing that is necessary to comply with a legal obligation (Article 6(1)(c)) or to perform a task carried out in the public interest (Article 6(1)(e)).
- Stakeholder interviews showed that during the previous ESF programming period of 2014-2020, consent was in particular used as a legal basis, especially in the collection of personal data from participants. Only one interviewee, from the Swedish Public Employment Service, mentioned that it uses another legal basis, based on its legal obligation to carry out ESF projects. It remains to be seen if this practice will be changed during the programming period 2021-2027, also due to the new provision under Article 17(6) ESF+ Regulation.
- National DPAs and courts have stressed the importance of clear and specific national provisions. Whilst Austrian and Spanish DPAs and courts did not (yet) provide any specific guidance regarding legal bases for the processing of data for ESF+ monitoring and evaluations, the Romanian DPA - ANSPDCP explained that due to the requirement for legislative transparency (foreseeability) the legal basis for such processing should be determined in a national regulatory act and not merely in a protocol which does not have a force of a legal document.

[176] Decision of 19 November 2020, GZ: 2020-0.743.659 (Vienna Contact Tracing Regulation), (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority)). https://www.dsb.gv.at/download-links/dokumente.html.

[177] Ibid., p. 27.

5.2. Reuse of personal data

This Section discusses the topic of further processing. To this end it looks at the rules on the processing of data for further purposes (Sub-section 5.2.1) and the processing of personal data for scientific purposes (Sub-section 5.2.2).

5.2.1. Processing of data for further purposes

One of the key data protection principles – the principle of purpose limitation in Article 5(1)(b) GDPR - requests that data must be processed **for specified, explicit and legitimate purposes** and must not be further processed in a manner that is incompatible with the purposes for which they were collected. It also implies that the purpose of processing should be determined at the time of data collection, as this will also determine the type of data to be processed. Any **reuse of data** needs to be assessed on a case-by-case basis and is only allowed if further purpose is compatible with the original one[178]. The **notion of compatible use** requires that in each situation where further use is considered, a distinction is made between additional uses that are compatible and those that remain incompatible (i.e., purpose compatibility test). EU case-law on the application of the purpose limitation principle in the context of secondary use of personal data is so far limited[179].

Article 6(4) GDPR establishes **criteria for determining the compatibility of further or secondary use** of personal data, largely following the guidelines of the WP29[180]. This provision makes clear that the question of further processing can only come up if the processing is not taking place on the basis of a consent or a law (Member State or EU legislation). Key factors to consider whether further processing on the basis of e.g. contract or legitimate interests can take place, include amongst others the following: (i) the link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (ii) the context in which the personal data have been collected and the reasonable expectation of the data subject as to their further use; (iii) the nature of personal data (any special categories); (iv) potential consequences or impact on data subjects; and (v) what safeguards are foreseen. In cases of compatible use, no further legal basis is required[181]. No relevant case-law of the CJEU on how to interpret this provision could be found.

In the case of processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e) GDPR), Union or Member State law could determine and specify the tasks for which the processing of personal data in registries is necessary. Similarly, the legal obligation based on a Union or Member State law (Article 6(1)(c) GDPR) could provide a legal basis for the processing of personal data in registries.

In the context of ESF+ monitoring and evaluations, the main reason behind the reuse of data is connected with the need to use existing data sets from national administrative

[178] Article 29, Data Protection Working Party. (2013). *Opinion 03/2013 on purpose limitation*.

[179] In the Österreichischer Rundfunk case the CJEU for example found that national law derogating from the purpose limitation principle is permissible only if the derogation and the secondary processing are proportionate to the aims it intends to achieve. See Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294 (Court of Justice of the European Union, Judgment of the Court, 20 May 2003). https://curia.europa.eu/juris/document/document.jsf?text=&docid=48330&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2465139.

[180] Article 29, Data Protection Working Party. (2013). *Opinion 03/2013 on purpose limitation*.

[181] If the controller however shares or further processes the data for purposes incompatible with the original purposes, then a new valid legal basis may be needed. See recital 50, GDPR.

registers (i) in case of counterfactual evaluations, where access to data of a control group (non-participants' data) is needed; (ii) in case of data concerning individual programme participants, in order to avoid the inefficiency of collecting information that already exist in national registers; or (iii) to avoid asking participants sensitive questions. In such a case, data have been collected initially for purposes other than the participation in ESF+ projects.

As discussed in Sub-section 5.1.2 above, **Article 17(6) of the ESF+ Regulation** touches upon the issue of access to existing data by stating that for the purpose of ESF+ monitoring and evaluation, Member States may consider granting access to personal data in their administrative registers. This provision further states that the legal basis for such a reuse of data should be in accordance with the GDPR provisions concerning a **legal obligation** (Article 6(1)(c)) or a performance of a task carried out in the **public interest** (Article 6(1)(e)).

The review of national data protection laws in Austria, Romania and Spain did not reveal such specific rules enabling reuse of existing data in national administrative registers. In a decision from 2017, the Spanish DPA held that provision of information by data subjects does not enable the controllers to use such information for purposes other than those for which the data was collected[182]. However, a legal basis for such reuse might be provided in further sector-specific national legislation.

Stakeholder interviews revealed that stakeholders in most Member States can access pre-existing datasets in their national administrative registers, although in some Member States they are only **granted access to anonymised data**. This depends on the national rules on the access to administrative data, implying that at least in some Member States a legal basis for such reuse of personal data exists.

Box 9: Example from the stakeholder interviews – Access to data from administrative registers

In some Member States, data from administrative registers could only be transmitted if data sharing agreements are in place (Ireland) or could only be transmitted in anonymised form so that the data subject can no longer be identifiable (Romania, Spain, Sweden).

It should be noted that there is a distinct difference between anonymised and pseudonymised data in data protection laws. While the former (anonymised data) does not qualify as personal data under the GDPR, the latter (pseudonymised data) is still personal data. **Anonymous information** is information which does not relate to an identified or identifiable natural person or information which is rendered anonymous in such a manner that the data subject is not or no longer identifiable. As such, **data protection law does not apply** to the processing of such anonymous information, including for statistical or research purposes[183]. **Pseudonymisation** is a technique to mitigate data protection risks by separating data from direct identifiers so that personal data can no longer be attributed to a specific data subject without additional information that is kept separately[184].

If when accessing data from the administrative registers national stakeholders are only provided access to anonymised data, this means that any reuse falls out of scope of the GDPR. If, however, data obtained from the administrative registers relates to identifiable

[182] Agencia Española de Protección de Datos (AEPD). Procedimiento Nº: AP/00023/2017

[183] Recital 26, GDPR.

[184] Article 4(5), GDPR.

individuals, the authority to obtain such data and use the data for a purpose that is incompatible with the initial purpose would need to have a legal basis for their reuse and also fulfil all other GDPR requirements (like the information obligation). **Article 11 GDPR** is also relevant in this regard as it governs processing that does not require identification, such as obtaining access to pseudonymised information. If in such cases the authority accessing such data can prove that it is not in a position to identify the data subject, the rights of data subjects in Articles 15 to 20 GDPR do not apply, unless the data subject wishes to exercise his or her rights under these provisions and for this purpose provides additional information enabling his or her identification[185]. The relationship between this provision and the obligation to inform data subjects of the secondary use of personal data[186] is discussed in Section 5.8.2 below.

5.2.2. Processing for the purpose of scientific research

Scientific research has traditionally been supported by the European Union (EU) and is a high priority for the European Commission. The GDPR provides for several provisions on scientific research in order to ensure that data protection laws do not impede its development. **Article 5(1)(b) GDPR** for instance states that secondary use for the purposes of scientific research shall not be considered to be incompatible with the initial purpose[187]. In short, the GDPR allows the reuse of data, including special categories of data, for the purpose of scientific research. For this reason, processing for scientific research entails the requirement of specific safeguards, as provided by **Article 89 GDPR**, which is discussed in detail below.

There is no universally agreed definition of scientific research[188]. Although the notion of 'processing for the purpose of scientific research' is not defined in the GDPR[189], **recitals 157 and 159** give some indication. For instance, the role of research is understood to provide knowledge that can in turn "*improve the quality of life for a number of people and improve the efficiency of social services*"[190]. Under the GDPR, "the processing of personal data for scientific purposes should be interpreted in a broad manner, including for example technological development and demonstration, fundamental research, applied research and privately funded research", as well as "studies conducted in the public interest in the area of public health"[191]. For the EDPS, the term 'scientific research' cannot be stretched beyond its common meaning "*a research project set up in accordance with relevant sector-related methodological and ethical standard, in conformity with good practice*"[192]. It is useful to highlight that recital 159, when providing that the processing of personal data for scientific purposes should be interpreted in a broad manner, gives the instance of applied research[193]. In light of the objective of the ESF/ESF+ evaluations to use scientific methods to address practical and specific questions, they could be deemed as instances of applied research.

The concept of research may not be limited to research institutions and universities. According to the EDPS Preliminary opinion, "*It also recommends that data processing 'take*

[185] Article 11(2), GDPR.

[186] Articles 13 and 14, GDPR.

[187] Other than this compatibility presumption, all other provisions in the GDPR, all other principles and obligations under the GDPR, such as the transparency obligation and the need for legal bases remain applicable.

[188] European Data Protection Supervisor. (2020). *A Preliminary Opinion on data protection and scientific research*. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, p. 9.

[189] European Data Protection Board. (2020c). *Guidelines 05/2020 on consent under Regulation 2016/679*.

[190] Recital 157, GDPR.

[191] Recital 159, GDPR.

[192] European Data Protection Board. (2020a). *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*. , para. 10.

[193] Recital 159, GDPR.

into account the EU's objective under Article 179(1) TFEU of achieving a European Research Area'. Therefore, not only academic researchers but also not-for-profit organisations, governmental institutions or profit-seeking commercial companies can carry out scientific research"[194]. This could be perceived as relevant in the context of ESF/ESF+ evaluations, which are frequently executed by consulting firms, on behalf of managing authorities, intermediary bodies, or other public institutions.

According to the Preliminary opinion of the EDPS[195], the scientific regime under GDPR should apply where each of the following **three criteria** is met: (i) processing of personal data; (ii) existence of relevant sectorial standards of methodology and ethics, including the notion of informed consent[196], accountability[197] and oversight[198]; and (iii) existence of the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily private interests. These criteria offer a rather restrictive definition of research, notably with the mention of informed consent as part of the second criterion. Indeed, it appears that the majority of research for social sciences, including ESF/ESF+ evaluations, would fail to align with this understanding of research due to their reliance on existing personal data already collected and stored in national databases rather than obtaining new personal data directly from data subjects based on informed consent. This contrasts with recital 157 GDPR which raises the importance of registry data for social sciences[199].

The second criteria identified by the EDPS mentions sectorial standards of methodology and ethics. In that respect, it is useful to mention the European Commission's guidance note, 'Ethics and Data Protection'[200], which addresses ethical considerations within the framework of EU research programmes, strives to raise awareness among the scientific community, particularly among recipients of EU research and innovation projects[201].

Pursuant to Article 44 of the CPR 2021, evaluations carried out can relate to effectiveness, efficiency relevance, coherence and Union added value, with the objective of improving the quality of the programme design and its implementation[202]. Taking into account the three EDPS criteria mentioned above, it could be argued that the evaluations carried out or commissioned by the managing authorities cannot be considered as scientific research in the meaning of the GDPR as they mainly aim at improving the design and implementations of the programmes evaluated, by assessing their performance, taking earlier expectations into account, as well as unintended or unexpected effects, to draw conclusions on whether particular programmes remain fit for purpose, should be adjusted or should no longer take place. The aims would thus be perceived as gearing towards ensuring the efficient and effective use of EU Funds, which would only have an indirect impact on enhancing the

[194] European Data Protection Supervisor. (2020). *A Preliminary Opinion on data protection and scientific research*. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

[195] Ibid., p. 12.

[196] This requires researchers to obtain the informed consent of all human participants in any of the research project and to disclose information about the study's purpose, risks, procedures as well as measures in the case of harms resulting from participation. The EDPS highlights that consent as a legal basis for processing must be freely-given, specific, informed and unambiguous, and this is to be distinguished from the informed consent concept, which applies to human participants in research. Ibid.

[197] The EDPS defines the accountability principle as requiring controllers to assess honestly and manage responsibly the risks inherent in their research projects. Ibid.

[198] The EDPS considers that an 'independent ethical oversight' implies that research involving human participants must be reviewed by independent ethics committees or Institutional Review Boards that examine whether the research is ethical, lawful and offers appropriate safeguards. Ibid.

[199] Recital 157, GDPR.

[200] European Commission. (2018a). *Ethics and data protection*.

[201] The European Commission Joint Research Centre has an Ethics Board to ensure compliance with ethical norms outlined in the manual. It could furthermore be argued that researchers in universities are knowledgeable about ethical considerations in research and some universities have established ethical guidelines. For instance the University of Reading, Science Po and Universidad Carlos III de Madrid.

[202] Article 44, CPR 2021.

overall knowledge and well-being of society. It might, however, also be argued that the effective and efficient use of public funds contributes to improving the wellbeing of society. Recital 157 provides that results of registry-based research offer solid, high-quality information that can inform evidence-based policy formulation and implementation, enhance the quality of life of a significant population and optimise the effectiveness of social services[203].

Furthermore, many evaluations of the ESF/ESF+ use counterfactual impact evaluation methods, aimed at determining a causal relationship between the programme and its outcome for participants. These evaluations are recognised as research within the academic and research community, undergoing peer review and often published in academic journals[204]. Although not all ESF/ESF+ evaluations are published in academic literature, they are still expected to adhere to rigorous scientific standards and employ robust research methods.

Therefore, depending on the understanding of the notion of research, not all evaluations conducted under the ESF/ESF+ can be classified as research, as some may be too narrow in scope, prove not to be using robust enough methodologies or have limited applicability to broader contexts.

Reflecting the strategic importance of the reuse of data under the EU's research policies, EU data protection law provides the so-called **presumption of compatibility**[205] according to which further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes. This presumption depends on **the requirement in Article 89(1) to ensure appropriate technical and organisational safeguards[206] to ensure in particular the principle of data minimisation**, for instance through the pseudonymisation and anonymisation of personal data whenever possible given the purpose of processing. The WP29 furthermore argued for ensuring that the data would not be used to support measures or decisions regarding any particular individual[207]. The presumption is not a general authorisation to further process data in all cases for historical, statistical or scientific purposes. Each case must be considered on its own merits and circumstances subject to appropriate safeguards.

Moreover, under Article 89 GDPR, when processing data for scientific research or statistical purposes, Union or Member State law may provide for **derogations** from data subjects' rights, subject to appropriate safeguards, to the extent that these rights are likely to render impossible, or seriously impair, the achievement of the specific purpose and such derogations are necessary for the fulfilment of those purposes[208]. When commenting on the creation of a central vaccination register and electronic vaccination passport in Austria, the national DPA also commented on the restriction of data subjects' rights, stating that any restriction must not only be necessary but also expressly stated in the law itself and require a more detailed statement of reasons in line with Article 89(2)[209].

[203] Recital 157, GDPR.

[204] See for instance Vooren, M., Haelermans, C., Groot, W., & Maassen van den Brink, H. (2019). The effectiveness of active labour market policies: A meta-analysis. *Journal of Economic Surveys*, *33*(1), 125-149. https://doi.org/https://doi.org/10.1111/joes.12269 which is based on a substantial body of evaluations found in the academic literature.

[205] Article 5(1)(b), GDPR.

[206] European Data Protection Board. (2021). *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf

[207] Data Protection Working Party. (2013). *Opinion 03/2013 on purpose limitation*. , p. 28.

[208] Article 89(2), GDPR.

[209] Opinion on Draft Amendment to the 2012 Health Telematics Act, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 17 January 2020). https://www.parlament.gv.at/PAKT/BEST/SN/index.shtml, p. 3.

The Austrian GDPR-implementing law (DSG) reserves its Member State discretion with respect to the reuse of data for specific purposes for two key situations: processing for archiving purposes in the public interest, scientific or historical research or statistical purposes, and during an emergency[210]. Romanian GDPR-implementing law (Law no. 190/2018) on the other hand uses the discretion provided in Articles 9(4) and 89 GDPR to further legislate in the area of processing for research purposes. To this end, Article 8 of the Law no. 190/2018 provides for a derogation from data subjects' rights in Articles 15, 16, 18 and 21 GDPR, subject to adequate safeguards in Article 89(1) GDPR. Spain's Organic Law 3/2018 also on several places regulates the processing of personal data for the purpose of research[211]. The Spanish DPA (AEPD) does not appear to analyse the technical aspects of measures in extensive detail, but instead focuses on ensuring that safeguards around the security of data and restrictions on reuse are maintained[212]. In particular, the AEPG provided approval for the contact-tracing app 'AsistenciaCOVID19' with reference to several national laws providing for the use of such data and to Article 89 GDPR (in light of the reuse for scientific research), requesting that specific safeguards should be implemented in relation to the system[213].

With respect to **consent**, the EDPB has on several occasions already noted that it could be seen as a valid legal basis for the processing of (special categories of) personal data, including for research purposes, if all conditions for an (explicit) consent are met. However, it may be questioned whether consent is an appropriate legal basis in research activities where there is a clear imbalance of power between the data subject and the controller (i.e., medical clinical trials)[214]. Recital 33 allows for consent to be given for certain areas of scientific research, if it is not possible to fully identify the scientific research purposes at the time of data collection. However, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked[215]. According to the EDPS, it is also important to **distinguish the requirement of informed consent** of participants in research projects involving humans and (explicit) consent as a legal basis under data protection law[216]. Even where consent is not seen as an appropriate legal basis under GDPR, informed consent could still serve as an appropriate safeguard of the rights of the data subject. However, it is still unclear under what conditions such informed consent might be considered as an appropriate safeguard[217]. For further analysis of the possible legal bases see Sub-sections 5.1.1 above and 5.3. below for consent. Possible exemptions for lifting the prohibition on processing of special categories of personal data are analysed in Sub-section 0 below.

[210] Sections 7 and 10, respectfully, DSG.

[211] For example, Section 2 of the 17th Additional Provision introduces a series of provisions (e.g. on reuse of personal data for health and biomedical research purposes, the use of pseudonymised data, restrictions of data subjects' rights) aimed at guaranteeing the proper development of research in the field of health, and in particular biomedical research, considering the undoubted benefits that it brings to society with the due guarantees of the fundamental right to data protection.

[212] See for example, COVID tracing apps, E/03346/2020, (2020a). https://www.aepd.es/es/documento/e-03346-2020.pdf and Train company (RENFE) and COVID data, E/03689/2020, (2020c). https://www.aepd.es/es/documento/e-03689-2020.pdf.

[213] COVID tracing apps, E/03346/2020, (2020a). https://www.aepd.es/es/documento/e-03346-2020.pdf.

[214] European Data Protection Board. (2019b). *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)*. and European Data Protection Board. (2020a). *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*.

[215] European Data Protection Board. (2021). *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf, para. 26.

[216] Ibid., para. 5 and European Data Protection Supervisor. (2020). *A Preliminary Opinion on data protection and scientific research*. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, pp. 19-20.

[217] European Data Protection Supervisor. (2020). *A Preliminary Opinion on data protection and scientific research*. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, ibid., p. 20.

Box 10: Key findings – Reuse of personal data

- If the processing is not taking place on the basis of a consent or a law (Member State or EU legislation), Article 6(4) GDPR establishes criteria for determining the compatibility of further or secondary use. In cases of compatible use, no further legal basis is required, and data could be reused.

- If the processing is based on a law, for instance, if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e) GDPR), Union or Member State law may determine and specify the tasks of a public authority in such a way that the processing of personal data in national registries can also be regarded lawful. The legal obligation based on a Union or Member State law (Article 6(1)(c) GDPR) may also be construed in a way that it provides for a legal basis for the processing of personal data in national registries.

- Apart from Article 17(6) of the ESF+ Regulation, no other Union provision could be detected that touches upon the issue of the reuse of data for the ESF+ monitoring and evaluation purposes. This provision gives Member States' guidance on the choice of legal bases for accessing data in national registers in accordance with Article 6(1)(c) or (e) GDPR.

- In order to obtain access to existing participants and non-participants' data, further national rules are needed. Stakeholder interviews revealed that several Member States' legislations facilitate such secondary use of data, albeit only in anonymised form.

- The definition of scientific research is not defined in the GDPR but recitals 157 and 159 provide some indication, notably that processing of personal data for scientific purposes should be interpreted broadly and that the role of research is understood to provide knowledge that can improve the quality of life for a number of people and improve the efficiency of social services.

- The concept of research may not be limited to research institutions and universities.

- There are arguments both for considering that evaluations carried out or commissioned by the managing authorities cannot be considered as scientific research and for considering that they can be, depending on the three criteria of the EDPS Preliminary opinion on data protection and scientific research, and on the scope and quality of the methodology of the evaluations in question.

- Article 5(1)(b) GDPR provides for a presumption of compatibility according to which further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes. Such processing requires appropriate technical and organisational safeguards to ensure in particular data minimisation, for instance through pseudonymisation and anonymisation.

- Under Article 89 GDPR, when processing data for scientific research or statistical purposes, Union or Member State law may provide for derogations from certain data subjects' rights, subject to appropriate safeguards, if such rights would seriously impair the achievement of the purposes and derogations are necessary to fulfil them.

5.3. Consent

In this Section consent as a legal basis is analysed. Sub-section 5.3.1 analyses the conditions for a valid consent, whereas Sub-section 5.3.2 analyses the conditions under which the consent could be a valid legal basis for the evaluation or monitoring of the ESF. Finally, Sub-section 5.3.3 considers the impact, if data that have been collected on the basis of consent migrate to another lawful legal basis.

5.3.1. Conditions for a valid consent

Consent is one of the six lawful bases to process personal data listed in Article 6 GDPR. In addition, *explicit* consent is one of the possible exemptions to lift the ban on processing of special categories of personal data in Article 9(2) GDPR[218]. Consent has been traditionally considered as the main legal basis for processing. However, according to the definition in the GDPR, the conditions for consent are very stringent.

Based on the definition in Article 4(11) GDPR consent means:

> *"[…] any **freely given**, **specific**, **informed** and **unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*

Generally, consent can only be an appropriate legal basis if a data subject is offered control and has a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When interpreting consent's requirements, recitals 32, 33, 42, and 43 GDPR as well as the EDPB's Guidelines 05/2020 on consent under Regulation 2016/679[219], which are built upon the existing WP29 Opinion 15/2011 on the definition of consent[220], are crucial sources of information.

Freely given implies a real choice and control for data subjects. Where data subjects would feel compelled to consent in order to avoid negative consequences (in particular in situations of imbalance between the controller and the data subject), the consent would not be seen as freely given and hence could be declared as not valid by the national DPAs or courts. Freely given also implies that consent cannot be bundled with acceptance of terms or conditions or that it is tied to the performance of a contract[221]. Consent should always be **specific**; if a processing operation has more than one purpose, data subjects should be able to pick and choose which purpose they accept, and consent should be given for all purposes[222]. The fact that the consent should be **informed** is a direct application of the principle of transparency. Minimum content requirements that should be provided to the data subject are: (i) the controller's identity; (ii) the purpose of each of the processing operations for which consent is sought; (iii) the type of data that will be collected and used; (iv) the existence of the right to withdraw consent; (v) the information about the use of the data for automated decision-making; and (vi) possible risks of data transmission[223]. All such

[218] The notion of special categories of personal data is elaborated in Section 5.3 below, whereas requirements for explicit consent are dealt with in this Sub-section.

[219] European Data Protection Board. (2020c). *Guidelines 05/2020 on consent under Regulation 2016/679*. These Guidelines present an updated version of the Article 29 Working Party Guidelines on consent under Regulation 2016/679.

[220] Data Protection Working Party. (2011). Opinion 15/2011 on the definition of consent. In.

[221] See in particular Article 7(4) and recital 43 GDPR.

[222] Recital 32, GDPR.

[223] European Data Protection Board. (2020c). *Guidelines 05/2020 on consent under Regulation 2016/679*. , paras. 64 and 65.

information should be provided in clear and plain language and should be clearly visible and distinguishable from other matters[224]. These requirements for consent are distinct from the separate information duties laid down in Articles 13 and 14 GDPR, which are discussed more thoroughly in Section 5.8. Finally, consent should be **unambiguous**, meaning that it requires a statement from the data subject or a clear affirmative act[225].

If the controller intends to collect and process **special categories of personal data**, requirements for consent are even more stringent as data subjects should provide ***explicit* consent**. The term 'explicit' refers to the way consent is expressed by the data subject, i.e., by an express statement of consent. EDPB's Guidelines provide some examples such as a written statement which can also be signed, filling in an electronic form, sending an email, uploading a scanned and signed document, using an electronic signature, using a two-stage verification or, in theory, even an oral statement of consent, which is recorded[226].

For other legal bases, consent must be given **before** starting to process data[227]. Furthermore, under Article 7 GDPR consent must be requested in a **transparent and fair way** (Article 7(2)), the controller should be able to demonstrate a data subject's consent (Article 7(1)) and consent should be **withdrawable at any time,** as easily as it was given (Article 7(3)).

5.3.2. Consent as a legal basis for processing data for ESF+ monitoring or evaluation

In the opinion of the EDPB, recital 43 of the GDPR clearly indicates that it is **unlikely** that public authorities can rely on consent for processing as whenever the controller is a public authority, there is often a **clear imbalance of power** in the relationship between the controller and the data subject. In most cases the data subject will have no realistic alternatives to accepting the processing (terms) of such a public body controller[228].

The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities. However, the use of consent as a lawful basis for data processing by public authorities is not *per se* excluded, especially if data subjects can refuse the processing of their data without any detriment or other negative consequences (e.g., substantial extra costs). Consent is not free in the case where there is any element of compulsion, pressure, or inability to exercise free will[229].

Consent as a legal basis is reversible, meaning that there remains a degree of control on the side of the data subject. The fact that consent **can be withdrawn** at any time makes it a rather cumbersome legal basis as processing after the withdrawal would be unlawful. Moreover, relying on consent does not legitimise the collection of data that is not necessary in relation to a specified purpose of processing, as basic data protection principles (e.g., purpose limitation and data minimisation) still apply.

National GDPR-implementing laws in Austria and Romania do not provide for any further requirements for a valid consent. The Austrian GDPR-implementing act for instance cross-refers to the text of the GDPR also with respect to legal basis of consent. **Spain** is an exception as in the context of processing of special categories of data, a mere consent is not sufficient to lift the prohibition on the processing under Article 9(2)(a) GDPR, when the

[224] See in particular Article 7(2) and recital 32 GDPR.

[225] See also recital 32 GDPR.

[226] European Data Protection Board. (2020c). *Guidelines 05/2020 on consent under Regulation 2016/679*. , paras. 93-98.

[227] Ibid. as well as Data Protection Working Party. (2011). Opinion 15/2011 on the definition of consent. In.

[228] European Data Protection Board. (2020c). *Guidelines 05/2020 on consent under Regulation 2016/679*.

[229] Ibid., para. 24.

principal purpose of this processing is to identify data subject's ideology, trade union membership, religion, sexual orientation, beliefs or racial or ethnic origin[230]. In a decision from 2017, the APED held that consent must be specific to the processing in question[231].

The decisions of national DPAs in Austria and Spain seem to be in line with the guidelines of the EDPB. When commenting on the Draft Federal Act amending the 1950 Epidemic Act, the Tuberculosis Act and the COVID-19 Measures Act, the Austrian DPA stated that consent is not an optimal legal basis for processing in the case of public authorities and that other legal bases (in the concrete case Article 9(2)(i) – processing for a public interest in public health) are more appropriate[232]. The DPA then added that if the final version of the act would continue to promote consent as a legal basis for processing, the prohibition on adverse consequences in instances of refusal to consent should be explicitly stated in the text[233]. To the contrary, the **ANSPDCP** in its general guidance on COVID-19 claimed that consent, where all requirements for a valid consent are met, could be used as a possible legal basis, provided that the appropriate safeguards are in place[234].

National research also demonstrates that in certain circumstances (for instance when processing involves certain types of data which could entail certain risks for data subjects' rights), consent can be the only valid legal basis. In Romania, copies of ID cards can only be processed with express consent of the data subject[235].

Due to such national specificities which go beyond GDPR rules, whether or not consent can be considered as an appropriate legal basis for processing of data for ESF+ monitoring and evaluations, will therefore depend on the circumstances of the case, in particular the types of data that need to be processed, the authority processing such data and the national rules appliable to such processing.

Box 11: Example from the stakeholder interviews – Consent

The interview answers show that especially when processing ESF participants' data directly from participants, the consent is most commonly used as a valid legal basis. In fact, all Member States but Sweden rely on consent as a legal basis when collecting data directly from project participants. Stakeholders commonly prepare special consent forms which are forwarded to participants in order to collect their personal information.

In case of counterfactual analysis, it is rarely that consent could be used as a legal basis to any processing of non-participants' data (examples include the use of data from refused participants as a control group, or the use of randomised control trials in which all potential participants give consent, but only some are then able to take part in a programme). However, in most cases of counterfactual analysis, the ESF+ authorities have access to

[230] Article 9(1), Organic Law 3/2018. However, Article 6 of the Spanish Organic Law 3/2018, which is a counterpart to Article 6(1)(a) GDPR, does not depart from the rules enshrined in the text and recitals of the GDPR.

[231] Agencia Española de Protección de Datos (AEPD). Procedimiento Nº: AP/00023/2017.

[232] Opinion Opinion on Draft Federal Act amending the 1950 Epidemic Act, the Tuberculosis Act and the COVID-19 Measures Act, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 16 August 2020 2020). https://www.parlament.gv.at/PAKT/BEST/SN/index.shtml, p. 2.

[233] Ibid., p. 2.

[234] Processing of health data, 18 March 2020, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/?page=Prelucrarea_datelor_privind_starea_de_sanatate&lang=ro.

[235] Decision no. 2952 of 18 May 2021, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

data from a control group, which was collected for a different purpose and usually made available to them in an anonymised form. This means that the ESF+ authorities do not have the possibility to contact individuals from a control group whose data are used for an evaluation.

5.3.3. Migration from consent to another legal basis

This Sub-section analyses if the processing that was done based on consent from participants by the original data collectors on the monitoring and evaluation process, can later be based on another legal basis, such as performance of a task based on the public interest in Article 6(1)(e) GDPR.

The answer to this question depends on the three potential scenarios:

- controller wants to migrate to a different legal basis due to problems with the validity of consent[236];
- data subject has withdrawn his or her consent;
- controller wishes to process data for another purpose and this time wants to choose a legal basis other than consent that better reflects the actual situation.

With respect to the first option – migration to another legal basis due to problems in the validity of consent - the EDPB already commented that **the controller cannot swap from consent to another legal basis retroactively** in order to justify processing. Whilst it is not excluded that certain processing operations could be based on several legal bases in Article 6 GDPR, the application of one or more legal bases must be established **prior** to the processing activity in relation to a specific purpose. Informing individuals that their data will be processed solely on the basis of consent, while actually some other lawful legal basis is relied upon, is in the opinion of the EDPB fundamentally **unfair** to individuals[237].

A different conclusion may be drawn in case of withdrawal of a consent or processing for a new/additional purpose. In these situations, the controller is no longer (withdrawal) or not yet (new/additional purpose) allowed to process personal data, meaning that processing can continue or start only if a new or a more appropriate legal basis is established. To this end the EDPB already commented that in instances where the data subject withdraws his or her consent and the controller wishes to continue to process the personal data on another lawful basis, which better reflects the situation, **such a change is possible but cannot be done silently**[238]. The principle of transparency requires that individuals are aware of the processing operations, in order to check whether processing is lawful and potentially exercise their rights. The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. As a result, any change in the lawful basis for processing must be notified to data subjects in accordance with the information requirements in Articles 13 and 14 GDPR (see below Section 5.8). Moreover, the controller should be able to explain to data subjects the likely impact of such a change on their rights and should not deceive the reasonable expectations of data subjects in line with principles of fairness and accountability[239].

[236] When processing was based on consent as a legal basis but not all elements for a valid consent were given. For instance, consent was not freely given due to an imbalance of power between the data subject and the controller.

[237] European Data Protection Board. (2020c). *Guidelines 05/2020 on consent under Regulation 2016/679*. , paras. 121-123.

[238] Ibid., paras. 58 and 120.

[239] European Data Protection Board. (2021). *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf, para. 38.

The above-mentioned EU-level analysis is also confirmed at national level by analysing decisions and cases relevant for processing of data for public purposes or by public authorities[240]. For instance, in a Vienna Contact Tracing Regulation case, the Austrian DPA has found that the collection of health data by the restauranteur in question had violated the principle of fairness by suggesting to customers that the provision of personal data was optional and based on consent[241]. The existence of a legal obligation as a legal basis to collect the data, particularly in circumstances of the restauranteur's misleading approach, was not sufficient to legitimise the processing[242].

Box 12: Key findings – Consent

- For consent to be seen as a valid legal basis it should represent a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- Although the requirements for a valid consent are relatively easy to understand, they might be difficult to implement, especially where there is an imbalance of power or where consent is a prerequisite to receive support or a benefit for the individual. In the opinion of the EDPB, recital 43 of the GDPR clearly indicates that it is unlikely that public authorities can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject.
- Moreover, consent can be revoked at any time, making it a rather cumbersome legal basis as processing after the withdrawal would be unlawful.
- National stakeholders usually rely on consent when collecting personal data directly from ESF/ESF+ project participants. In case of counterfactual analysis, it is conceptually impossible to use consent as a legal basis to any data processing, as the ESF+ authorities do not have an opportunity to contact individuals from a control group whose data will be used for this evaluation.
- If problems in the validity of consent occur, national authorities cannot migrate from consent to another legal basis retroactively in order to justify processing.
- Only in certain cases can consent be replaced by another legal basis, albeit not silently as data subjects need to be informed of such a change. This could apply in case of withdrawal of a consent or processing for a new/additional purpose.

5.4. Special categories of personal data

This Section deals with special categories of personal data ('sensitive data'). Sub-section 5.4.1 explains if special categories of personal data are processed for the purposes of ESF+

[240] As no cases on processing of personal data for ESF+ purposes have been identified in the three Member States selected for the in-depth review (Austria, Romania and Spain), the analysis has focused on cases of processing of data by public sector or for public purposes.

[241] Decision of 19 November 2020, GZ: 2020-0.743.659 (Vienna Contact Tracing Regulation), (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority)). https://www.dsb.gv.at/download-links/dokumente.html, p. 28.

[242] Ibid., p. 28.

monitoring and evaluations, Sub-section 0 analyses the applicable exemptions for lifting the prohibition on processing special categories of personal data in Article 9(2) GDPR, including the possibility to rely on 'scientific research', while Sub-section 5.4.3 explains some further challenges to the processing of special categories of personal data at the Member State level.

5.4.1. Special categories of personal data in the context of ESF+ monitoring or evaluations

Data that relate to the health, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, or biometric data of individuals are considered **special categories of personal data ('sensitive personal data')** for the purposes of the GDPR (Article 9(1)). This may include personal or even non-personal data that inadvertently reveal one of these categories (e.g., attendance at a particular health clinic or religious event[243], dietary requirements). The EU legal framework both under the old (2014-2020) and the new programming period (2021-2027) requires Member States and their managing authorities to collect for ESF/ESF+ monitoring and evaluation purposes and managing authorities to report a range of personal information about participants of ESF/ESF+ programmes (such as gender, age, labour market status, level of education) as well as beneficial owners of the recipients of EU funding[244], including some variables that are considered as special categories of personal data, such as those related to disability or ethnicity. In fact, Annexes to the ESF+ Regulation refer to several items which result in collection of special categories of personal data such as: disability, foreign background, minorities (including marginalised communities, such as Roma people).

However, values for indicators listed in the ESF+ Regulation that could result in processing of special categories of personal data, could be determined based on **informed estimates** provided by the beneficiaries. Member States **can** rely on informed estimates for processing of special categories of personal data in Annex I, Section 1.2 of the ESF+ Regulation along with indicators under Annex II and **shall** rely on informed estimates for processing of the common result indicators listed under Annex III (sensitive information). This is different for other indicators, which need to be collected for all participants (e.g., common output indicators and the common immediate results indicators listed in Annex I of the ESF+ Regulations), or which may be collected for a subset of participants, by using a sampling approach (i.e., data for the common longer-term result indicators for participants under Annex I, Section 4 of the ESF+ Regulation). However, whether informed estimates completely eliminate the need to process special categories of personal data depends on the method chosen to produce informed estimates as some methods, especially the method of 'sampling approaches' still rely on the collection of individuals' data[245].

In order to understand the full extent of the collection of special categories of personal data for the purpose of ESF+ monitoring or evaluations, one would also need to review the national-level legal documents and procedures for the establishment and collection of data necessary for monitoring and evaluation[246].

Stakeholder interviews show that for the ESF programming period 2014-2020 beneficiaries have been collecting special categories of personal data in most of the Member States

[243] Bodil Lindqvist v Sweden, ECLI:EU:C:2003:596. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101

[244] Annex XII CPR 2021 for instance requires the collection of information on the beneficiaries of EU fundings, which could also be natural persons.

[245] ESF+ Data Support Centre. *Note on Informed Estimates, July 2020 (revised version)*.

[246] See for example Articles 44(4) and 69(4), CPR 2021.

covered by this study. For instance, interviewees from Austria, France, Ireland, Poland, and Sweden explicitly said that they have collected special categories of personal data from the participants. However, in some Member States processing of special categories of personal data was not always possible. This depended on the type of stakeholders or the type of data.

Box 13: Example from the stakeholder interviews – Special categories of personal data

Stakeholders from Germany, Italy, Romania and Spain most commonly complained that they were unable to process special categories of personal data. Furthermore, although Irish stakeholders mostly claimed that they were able to process such data, one intermediary body mentioned that they were unable to collect them. Interviews with different Spanish stakeholders (i.e., managing authorities, external evaluator) revealed that special categories of personal data often could not be processed or could only be processed with explicit consent of everyone involved. In Germany, it seems that stakeholders were unable to process certain types of personal data, such as data regarding minorities and disabilities.

5.4.2. Possible exemptions for lifting the prohibition to process special categories of personal data for the ESF+ monitoring or evaluations

Processing of special categories of personal data should fulfil conditions for a lawful legal basis in Article 6 GDPR. Moreover, any processing of such personal data also requires an exemption for lifting the prohibition on processing of special categories of personal data in Article 9(1) GDPR. As processing of special categories of personal data represents a greater interference with data subjects' rights, in many situations lifting the prohibition requires detailed and clear Union or Member State legislation, including more specific safeguards to protect individuals' personal data.

Processing of special categories of personal data is in general prohibited (Article 9(1) GDPR), unless the controller can base its processing on one of the **10 grounds or exemptions for lifting the prohibition** in Article 9(2) GDPR, which are:

(a) explicit consent for one or more specified purposes (unless Union or Member State law does not allow a data subject to lift the prohibition to process personal data);

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment and social security and social protection law;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person, where such a person is incapable of giving consent;

(d) processing is carried out in the course of legitimate activities by a foundation, NGO or similar organisation and limited to the members or former members of the body and not disclosed outside of that body;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims;

(g) processing is necessary for substantial public interest based on Union or Member State law;

(h) processing is necessary for preventive or occupational medicine, medical purposes or to manage health or social care systems;

(i) processing is necessary for public interest in the area of public health;

(j) processing is necessary for archiving, in the public interest, scientific or historical research or statistics.

Similarly, as in the case of legal bases in Article 6 GDPR, the list of exemptions from the general prohibition on processing of special categories of personal data in Article 9 is **exhaustive**. For the purpose of this study **four grounds or exemptions** for lifting the prohibition on processing in Article 9 are of particular relevance: Article 9(2)(g) (processing for reasons of substantial public interest), Article 9(2)(h) (processing for the purpose of preventive or occupational medicine or management of health or social care systems), Article 9(2)(i) (processing for the public interest in the area of public health), and Article 9(2)(j) (processing for archiving, scientific and historical research, and statistics). All of these exemptions relate to areas associated with the "public interest" or official function and apply regardless of whether the processing is carried out by public sector bodies[247]. **Article 9(2)(g)**, as opposed to its counterpart Article 6(1)(e), provides for an exemption for lifting the general prohibition when processing is necessary for reasons of ***substantial*** **public interest**[248]. Imposition of the condition 'substantial' imposes a higher threshold, although the GDPR does not provide for a definition of this legal standard. For a legislative act to satisfy an exemption for lifting the general prohibition it must be, cumulatively: proportionate to the aim pursued, respectful of the essence of the right to data protection and providing suitable and specific measures to safeguard the fundamental rights and interests of data subjects. **Article 9(2)(h)** creates an exemption from the general prohibition for processing special categories of personal data for reasons of **medicinal purposes**, which include preventive or occupational medicine, the assessment of the working capacity of the employee or medical diagnosis or **management of health or social care systems**, which includes the provisions of health or social case or treatment. As such, it provides for processing special categories of personal data in the context of the provision of healthcare services, including at the individual as well as the systemic level. Article 9(3) GDPR adds a condition that such processing should be done by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy or rules established by national competent bodies. **Article 9(2)(i)** enables processing in **public interest in the field of public health**. By reference to Regulation (EC) 1338/2008 on Community statistics on public health and health and safety at work[249], recital 54 GDPR clarifies that "public health" should be interpreted broadly. These two provisions provide a list of possible examples, which may guide a Member State's legislators, national DPAs or processing entities when judging whether processing may fall within this section. Finally, **Article 9(2)(j)** allows for the processing that is necessary for archiving purposes in the public interest, **scientific or historical research purposes or statistical purposes**.

[247] Article 9(2) GDPR and recitals 52 – 55 that contain further explanation of these sections do not specify that the entity must be a public sector body.

[248] For a more detailed discussion on the legal concept of "public interest", see Taylor, M. J., & Whitton, T. (2020). Public Interest, Health Research and Data Protection Law: Establishing a Legitimate Trade-Off between Individual Control and Research Access to Health Data. *Laws*, *9*(1). https://doi.org/10.3390/laws9010006

[249] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work.

Whilst all aforementioned GDPR provisions require **certain safeguards** to be in place, exemptions in Article 9(2)(g), 9(2)(i) and 9(2)(j) require them to be contained within the text of any implementing legal instrument ('suitable and specific measures to safeguard interests of the data subject')[250]. The exemption in Article 9(2)(j) goes even further as it requires also the incorporation of Article 89(1) safeguards that include technical and organisational measures.

As elaborated above, all of the stipulated exemptions from the general prohibition on processing special categories of personal data in Article 9 GDPR **require additional Union or Member State legislation** for processing. Moreover, Member States may maintain or introduce further conditions, including limitations (for example data localisation requirement), with regard to the processing of genetic data, biometric data or data concerning health[251] or provide for further safeguards and derogations from data subjects' rights in the case of processing for archiving purposes in the public interest or for scientific or historical research purposes or statistical purposes [252]. This implies that the choices made in Member State laws can have a considerable impact on the exemptions that must be relied on when processing special categories of personal data.

The EU legal framework applicable to the current ESF+ programming period (2021-2027) on several provisions mentions that processing of monitoring data should be in line with the GDPR principles (see in particular Article 4 CPR 2021 and recital 33 ESF+ Regulation).

The analysis of the national implementing laws of the three Member States studied in-depth, demonstrates that the discretion provided by the GDPR has been interpreted in several different ways by the Member States, each adapting the provisions to its own legal system. Table 13 below shows if Member States have chosen to exercise their discretion in Article 9(4) and introduce further conditions in relation to the exemptions in Article 9(2)(g)-(j). 'Yes' means that Member States have decided to introduce such further conditions, while 'No' means that national GDPR laws do not further legislate in this area.

Table 13: Matrix of three Member States decisions to exercise discretion in key exemptions

Member State	Article 9(2)(g) – substantial public interest	Article 9(2)(h) – preventive or occupational medicine or management of health or social care systems	Article 9(2)(i) – public interest in public health	Article 9(2)(j) - archiving, scientific and historical research, & statistics	Article 9(2) – genetic data, biometric data or data concerning health
Austria	Yes*	No	No	Yes	No
Romania	Yes	No	No	Yes	Yes
Spain	Yes	Yes	Yes	Yes	Yes

[250] On contract, the text of Article 9(2)(h) only requires observance of safeguards of professional secrecy. See Article 9(3), GDPR.

[251] Article 9(4), GDPR.

[252] Article 89, GDPR.

** It is unclear if the competence of Austria to legislate in the area of emergencies (Article 10 DSG) falls outside of the scope of Union law in line with recital 16 GDPR or whether emergency state is seen as an extension of the (substantial) public interest ground.*

The national data protection law of **Austria** (DSG) reserves its Member State discretion for only two key situations: processing for archiving purposes in the public interest, scientific or historical research or statistical purposes (Article 9(2)(j) GDPR), and during an emergency (possible Article 9(2)(g) GDPR)[253]. Except for this, the DSG does not provide for any general rules for the processing of special categories of personal data[254]. When comparing Article 9(2)(j) with Austria's requirements for research and statistical processing in Section 7 DSG, we see that there are **additional restrictions** on the entity carrying out processing (either at the controller's premises or by an entity whose 'reliability is credible'. It is also interesting to note that the use of identifiable data for such purposes (or at least identifiable data that has not been pseudonymised) may only be undertaken if at least one of the additional safeguards is met: (i) the subject's consent (which is an additional safeguard); (ii) a specific legal provision providing for the processing; or (iii) where the DPA gives a permit[255]. The second area of Member State discretion exercised by Austria is the provisions of Section 10 on processing personal data in an emergency, which could be considered to represent a case of 'substantial public interest' under Article 9(2)(g). The Austrian DPA concluded in September 2021 that the COVID-19 pandemic should be considered as an 'emergency' for the purposes of this Section[256]. Processing of large amounts of special categories of personal data by a public authority requires a data protection impact assessment as decided by the Austrian DPA[257].

Spain has on several occasions exercised its discretion with respect to the processing of special categories of personal data. The processing of data based on exemptions in Article 9(2)(g), (h) and (i) must be covered by a rule with the rank of a Spanish law, and this law could establish additional requirements regarding security and confidentiality[258]. Deciding on the constitutionality of the General Election Regime Law, the Spanish Constitutional Court in 2019 held that the processing of special categories of personal data is one of the areas in which the GDPR has expressly recognised Member States' "margin of manoeuvre". As the use of special categories of personal data is likely to compromise the dignity, freedom and free development of the personality more directly, the need to have adequate guarantees is even more important. The Court also pointed out that due to an obligation that such exemptions must be covered by a law, any deficiencies in national legislation cannot be filled through conformity interpretation of the normative acts or guidelines by the national DPA [259]. The Organic Law 3/2018 also regulates several aspects of data processing at the workplace, including the use of video surveillance (CCTV) and sound recording devices at work, and geolocation technology, and has an extensive section to regulate the processing of health data[260]. The latter includes an exhaustive list of existing legislation that may be deemed acceptable national laws for the purposes of Article 9 GDPR. Notably in the field of health research, the use of pseudonymised data is broadly permissible, with additional safeguards for non-pseudonymised data including a favourable report of the

[253] Sections 7 and 10, respectfully, DSG.

[254] Bird&Bird. *GDPR Tracker - Special rules for special categories of data*. Retrieved 12 October 2022 from https://www.twobirds.com/en/capabilities/practices/privacy-and-data-protection/general-data-protection-regulation/gdpr-tracker/special-categories-of-personal-data.

[255] Review of publicly available sources did not allow to identify such DPA's approvals. Hence, it is difficult to comment upon the effect of this safeguard in practice.

[256] Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority). (2021). *Information from the data protection authority on the coronavirus (Covid-19)(Information der Datenschutzbehörde zum Coronavirus (Covid-19))*. https://www.dsb.gv.at/download-links/informationen-zum-coronavirus-covid-19-.html.

[257] DPA's Opinion on Federal draft law amending the 1992 Student Support Act (StudFG Novelle), GZ: D055.654 2022-0.308.733 (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority)).

[258] Article 9(2), Organic Law 3/2018.

[259] Judgment 76/2019 of 22 May 2019, BOE [Official Gazette] number 151, of 25 June 2019 (Constitutional Court).

[260] 17th Additional Provision, Organic Law 3/2018.

ethics committee for the research and consent of the data subject (unless the research has exceptional significance and seriousness for public health). The Spanish DPA recently held that a regulation relating to processing health data for the purpose of COVID-19 certificates was not sufficient to legitimise the processing (contact tracing clubs) as it did not have 'the force of law' as required by its GDPR-implementing legislation and lacked the rank to interfere with fundamental rights[261].

Finally, **Romania** also used the opportunity to further implement certain GDPR provisions on the processing of special categories of personal data. Law no. 190/2018 for instance provides for several exemptions from the ban on processing of special categories of personal data, largely drawing upon the text of GDPR, including in relation to genetic, biometric and health data (Chapter II, Article 3), and employment (Article 5) and tasks in the substantial public interest (Article 6). In each case, the national provisions refer to the GDPR, with reference to additional safeguards to be determined on the basis of the nature of the processing involved.

The processing of special categories of personal data, as with the processing of any personal data, **requires a legal basis under Article 6 GDPR**. **In addition, an applicable exemption, allowing the processing despite the general prohibition under Article 9(1), is required**[262]. When processing special categories of personal data, all general principles and rules of the GDPR apply. Based on the text of the GDPR, it could be argued that where exemptions in Article 9(2) correlate with legal bases in Article 6(1), while offering an even stricter and better protection (i.e., exemption of *explicit* consent, vital interest of a person *physically or legally unable to give consent*, *substantial* public interest), such exemptions subsume the corresponding legal basis.

5.4.3. Overcoming national particularities when processing certain special categories of personal data

The Technical Specifications[263] pose a question on **how to collect participant data for health-related ESF+ interventions** (for example supporting HIV or COVID-19 patients) without breaching the GDPR. As seen above, the processing of special categories of personal data, such as health data, require both a legal basis in Article 6 GDPR – most probably Article 6(1)(c) or (e) - and an exemption from the prohibition of processing special categories of personal data in Article 9(1) GDPR. Article 9(2)(i) - processing for the public interest in the area of public health, which is more specific than the general exemption of 'substantial public interest' in Article 9(2)(g), and (j) - processing for archiving, scientific and historical research, and statistics seem the most appropriate choices. Exemption in Article 9(2)(h) seems to be reserved to health professionals and healthcare institutions.

Article 9(2)(i) can be used if processing is necessary for reasons of public interest in the area of **public health** without explicit consent of the data subject, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. The concept of 'public health' mentioned in Article 9(2)(i) should be interpreted as defined in the Regulation (EC)

[261] The Spanish Data Protection Agency Procedimiento N.º E/06406/2020, (2021a). https://www.aepd.es/es/documento/e-06406-2020.pdf

[262] The EDPB indicated that it expects both a legal basis under Article 6 and an exemption from the prohibition on special categories of personal data processing in Article 9 to be in place. See European Data Protection Board. (2019c). *Opinion 3/2019 concerning theQuestions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))*. https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en.

[263] Terms of Reference, p. 13.

1338/2008 on Community statistics on public health and health and safety at work[264]. Whilst all aforementioned provisions in Article 9(2) require suitable safeguards to be in place, Article 9(2)(i) requires them to be contained within the text of any EU or national implementing legal instrument.

The exemption in **Article 9(2)(j)** enables, inter alia, the processing of data for **scientific research or statistical purposes**. In combination with Article 89(1), this exemption makes even more detailed legislative demands on EU and Member States, as it requires any implementing legal instrument to provide safeguards that include technical and organisational measures, with additional specific examples of such measures.

In the absence of specific Union laws, it is necessary to look at **national GDPR implementing laws as well as other national (sectorial) laws** to identify the provisions which make the collection of health data of HIV and COVID-19 patients. Additionally, **opinions of national DPAs** would need to be taken into account.

When discussing the collection of data on COVID-19 patients, each national DPA has to interpret the provisions of the GDPR in light of its national government's response to the pandemic. For instance, Romania's DPA advised its government to preserve the role of the public authority responsible for collecting census data when emergency legislation proposed the extension of the power to collect census data to other processors during the COVID-19 pandemic[265]. The DPA advised that the framework service contract for the census should include a specific provision to the effect that the National Institute of Statistics and its territorial entities would remain the controller of any census data processed.

Another question on national particularities evolves around the **problem of 'prohibited' data**[266] such as the situation in **Austria** where a managing authority's obligation to report certain participants' data related to ethnicity clashes with participants' fundamental freedom of confession ('*Prinzip der Bekenntnisfreiheit*'). Based on Article 3(1) of the Council of Europe Framework Convention for the Protection of National Minorities[267] and Section 1(3) and (4) of the Austrian Ethnic Groups Act[268], no person should be obliged to declare his or her ethnicity. In the opinion of the Federal Austrian Chancellery from 26 November 2021[269], these provisions request that situations where members of minorities would be required to confess whether they belong to an ethnic group or not should be avoided. Stakeholder responses show that during the past funding period (2014-2020) this problem has been mitigated in a way that the decision on whether to collect the minority membership indicator was left to participants who could leave this question unanswered. A similar approach has also been taken by the Austrian Ministry of Labour and Economy[270] for the current programming period 2021-2027. The latter advises that due to the principle of freedom of

[264] See recital 54, GDPR.

[265] Review of draft Government Emergency Ordinance no. 19/2020 on the draft Government Decision on the budget and expenditure categories for the population and housing census in Romania in 2021 as well as the establishment of measures on the implementation of certain provisions of Government Emergency Ordinance no. 19/2020, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro.

[266] Terms of Reference, p. 13.

[267] Framework Convention for the Protection of National Minorities. https://www.coe.int/en/web/conventions/cets-number-/-abridged-title-known?module=treaty-detail&treatynum=157

[268] Federal Act of 7 July 1976 on the Legal Status of Ethnic Groups in Austria (Ethnic Groups Act) (Volksgruppengesetz). https://www.jusline.at/gesetz/vgg/gesamt

[269] Federal Chancellery. Inquiry on the Definition of the Term "Minority" in Austria, Statement (Bundeskanzleramt, Anfrage zur Definition des Begriffes "Minderheit" in Österreich) Nr. 2021-0.802.012, from 26 November 2021.

[270] Definitions of the common ESF+ (and JTF) indicators (output and result indicators) of the programme period 2021-2027 (Definitionen der gemeinsamen ESF+ (und JTF) Indikatoren (Output- und Ergebnisindikatoren) der Programmperiode 2021-2027) (Austria).

confession and since data on ethnicity are special categories of personal data, participants can decide not to provide such data[271].

This implies that in Austria, processing of ethnicity data requires consent of an individual. Whether and how to establish a valid legal basis for processing such information would again depend on the **analysis of national discretion** taking into account national legalisation, opinions of the DPA and jurisprudence of national courts. Analysis of Articles 6 and 9 GDPR shows that, due to Member States' discretion, further conditions for processing (special categories of) personal data might exist at the national level. In Austria, for example, Section 7(1) of the DSG allows for processing of **all** personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, if the goal is not to obtain results in a form relating to a specific data subject and pursuant to one of the following conditions: (i) if personal data are publicly accessible; (ii) if the controller has lawfully collected such data for other research projects or other purposes; or (iii) if data are pseudonymised for the controller and the controller cannot establish the identity of the data subject by legally permissible means. The use of identifiable data for such purposes (or at least identifiable data that has not been pseudonymised) may however only be undertaken if at least one of the additional conditions is met[272]: (i) a specific legal provision; (ii) a consent of the data subject (which is an additional safeguard); or (iii) a permit of the Austrian DPA[273]. Additionally, if special categories of personal data are to be collected (such as data revealing ethnicity), an important public interest in the research project must exist and personal data must be processed at the premises of the controller who commissioned the research project. The processing can only be done by persons who are subject to a statutory obligation of confidentiality regarding the subject matter of the research project or whose reliability in this respect is credible.

The fact that the obligation to process certain personal data can collide with participants' fundamental rights and freedoms is also recognised in the ESF+ Regulation. Recital 33 of the ESF+ Regulation specifically calls for respect of dignity and privacy of the individuals. To this end this recital provides that, to avoid any stigmatisation, the persons receiving food and/or basic material assistance should not be required to identify themselves when receiving the support and when taking part in surveys targeting the most deprived persons who have benefitted from the ESF+ support under a specific objective (m)[274].

Lastly, the **usage of informed estimates** could circumvent the need for processing certain (special categories of) personal data. As explained in Sub-section 5.4.1, informed estimates in the 2021-2027 programming period are foreseen as a method to report on operations and indicators under Section 1.2 of Annex I[275] and Annex II[276] of the ESF+ Regulation and need to be provided for the two common output indicators under Section 1.2 of Annex III[277] and all common result indicators. MAs are free to choose the approach on how to produce informed estimates. This would most commonly entail a combination of techniques such as sampling approaches, proxies and educated guess from informed actors involved[278]. While some of these methods to produce informed estimates do not presume collection of data

[271] Ibid.p. 8.

[272] Section 7(2), DSG.

[273] Review of publicly available sources did not allow to identify such DPA's approvals. Hence, it is difficult to comment upon the effect of this safeguard in practice.

[274] Recital 33, ESF+ Regulation.

[275] These are common output indicators which track the number of participants with disabilities, third country nationals, participants with a foreign background, minorities, homeless, and participants from rural areas.

[276] These are common output indicators which track the age group of the individuals (Section 1.1), as well as number of participants with disabilities, third country nationals, participants with a foreign background, minorities, and homeless (Section 1.2).

[277] Share of food donations and share of ESF+ support over total food distributed.

[278] ESF+ Data Support Centre. *Note on Informed Estimates, July 2020 (revised version)*. p. 3.

from individuals, the sampling approach still relies on data collected from participants[279]. If usage of informed estimates could simplify data collection to the extent that certain indicators could be reported without the need to collect information on individual participants, such processing would fall outside the scope of the GDPR.

Box 14: Key findings – Special categories of personal data

- Special categories of personal data ('sensitive personal data') for the purposes of the GDPR (Article 9(1)) are any data that relate to the health, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership as well as, genetic data, or biometric data of an individual when such data are processed uniquely for the purpose of identifying that individual.

- The EU legal framework both under the old (2014-2020) and the new programming period (2021-2027) requires stakeholders to process a range of personal information about participants of ESF/ESF+ programmes. Some of the indicators might require collection of data that are considered as special categories of personal data, such as those related to disability or ethnicity. However, beneficiaries are allowed to determine the values for such indicators based on informed estimates. In such a way, the need for processing certain types of special categories of personal data could be avoided. This would, however, depend on the method chosen to produce informed estimates.

- Despite this requirement, stakeholder interviews in some Member States show that processing of special categories of personal data was not always possible in 2014-2020. Stakeholders from Germany, Italy, Romania and Spain most commonly complained that they were unable to process special categories of personal data. Interviews with different Spanish stakeholders (i.e., managing authorities, external evaluator) for example revealed that special categories of personal data could often not be processed or could only be processed with explicit consent of everyone involved. In Germany, it seems that stakeholders were unable to process certain types of personal data, such as data regarding minorities and disabilities. In Ireland, one intermediary body mentioned that special categories of personal data cannot be shared, accessed or reused without a data sharing agreement and data protection impact assessment. Moreover, the Italian DP**O** stated that special categories of personal data are excluded from the scope of reusable public sector information.

- The processing of special categories of personal data, like the processing of any personal data, requires a legal basis under Article 6 GDPR. In addition, processing of special categories of personal data requires an exemption allowing the processing despite the general prohibition under Article 9(1) GDPR. For the purpose of this study exemptions in Article 9(2) letters (g), (h), (i) and (j) are of particular relevance as they relate to areas associated with the 'public interest' or official function and apply regardless of whether the processing is carried out by public sector bodies.

- Collection of participants' data for health-related ESF+ interventions (e.g., supporting HIV or COVID-19 patients) would very likely entail processing of special categories of personal data. In order to collect such data, national authorities should avoid their processing activities relying on on explicit consent

[279] Ibid.pp. 4-8.

but should consider the possibility of using other exemptions to lift the ban on processing, e.g. Article 9(2)(i) on the processing of data for reasons of public interest in the area of public health or, possibly in some cases, Article 9(2)(j) on processing of data for scientific research or statistical purposes. This would depend on the national legislation in place.

- In Austria, the obligation to collect data related to ethnicity collides with the participants' freedom of confession. As a result, the collection of the minority membership indicator is only possible based on consent of an individual, who can also decide not to reveal his or her ethnicity.

5.5. Transmission of data

Analysis of data transmissions focuses on two elements: the definition of a data transmission (Sub-section 5.5.1) and the legal obligations arising from the EU law when administrative data are transmitted for evaluations or monitoring (Sub-section 5.5.2).

5.5.1. Definition of a data transmission

Data transmission in the context of this study is understood as exchanging data between different actors responsible for ESF+ monitoring or evaluations (i.e., sending or forwarding data on one hand and receiving or accessing data on the other hand).

Based on desk research and stakeholder interviews, two types of data transmission should be considered:

- when data holders transmit existing public sector datasets (i.e., administrative data) to managing authorities: or
- when managing authorities transmit personal data from pre-existing public authorities' databases to ESF evaluators[280].

While data holders and managing authorities are public bodies/authorities, ESF evaluators could be either public or private sector contractors or statistical or academic experts.

5.5.2. Legal obligations arising from the EU and national law

Under the GDPR, each action performed in relation to data is considered 'processing'[281]. Hence, transmission of data falls under the definition of a **processing operation** which, pursuant to Article 4(2) of the GDPR, means any operation or a set of operations which is performed on personal data or on sets of personal data, whether or not by automated means[282]. The act of transmission entails two sets of processing operations – the act of granting access to personal data and the act of receiving such data. As any processing of

[280] Transmission of data for the purpose of ESF/ESF+ reporting from MAs to the EU does not include any personal data as only aggregated data is reported.

[281] Data processing means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, access, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, linkage, dissemination or otherwise making available, alignment or combination, restriction, erasure or even destruction (Article 4(2) GDPR).

[282] Article 4(2), GDPR.

personal data should be lawful, meaning that it should have a clear legal basis[283] in line with the principle of lawfulness, **both the access to personal data as well as the receipt of personal data should be based on one of the legal bases** in Article 6(1) and be also allowed under Article 9(2) in case of transmission of special categories of personal data.

Transmitting data from one entity to another should also comply with all other **basic data protection principles** in Article 5 GDPR. For instance, the **principle of fairness and transparency** requires that personal data should not be forwarded if this could be detrimental, discriminatory, unexpected, or misleading for the data subject and that data subjects should be informed about such transmissions (for the obligation to inform data subjects see Section 5.8 below)[284]. The **principle of purpose limitation** requires that data can only be processed for specified, explicit and legitimate purposes and must not further be processed in a manner that is incompatible with the purposes for which they were collected. Hence, the reuse of data based on the same legal basis should be compatible with the original purpose (see also above under Sub-section 5.2.1)[285]. Only personal data that are correct and up to date[286] as well as data that are adequate, relevant and limited to what is necessary in relation to the purpose shall be transmitted[287]. Also relevant is the **principle of integrity and confidentiality**, which among other things requires that personal data is transmitted in a secure way that prevents unauthorised or unlawful processing or accidental loss, destruction or damage of personal data[288].

In line with the **principle of accountability**, the controller is responsible to ensure compliance with data protection principles and obligations in the GDPR, even in cases of onward transmission. This implies that the responsible person needs to take all the necessary measures to observe principles and obligations in the applicable EU and national legislation and have in place necessary internal technical and organisational measures to be able to demonstrate compliance with these principles and obligations[289].

As GDPR is an enabling Regulation, in the sense that it provides a general legal framework of the processing of personal data, further Union and Member State law would need to be analysed in order to conclude on the individual obligations of actors involved in transmissions of data for ESF+ purposes.

Although domestic data protection laws in Austria, Romania and Spain do not depart from the wording of the GDPR with respect to this topic, national DPAs have on several occasions provided interpretation of the GDPR provisions governing the transmission of data.

In its Opinion on draft legislation for e-ID, the Austrian DPA explained that where public authorities are involved, **any transmission of data should be governed by specific legislation**[290]. The DPA further suggests that the specific personal data categories (first and last name, date of birth, etc.) and the respective purposes for the transmission of the listed categories of personal data should be covered by law. The latter should be as specific as possible in order to comply with the requirements of the GDPR and national data protection legal framework. In another opinion on the draft Federal Act amending the Federal Statistics

[283] Article 2, and definitions in Article 4, GDPR.

[284] Article 5(1)(a), GDPR.

[285] Article 5(1)(b), GDPR.

[286] For principle of accuracy see Article 5(1)(d), GDPR.

[287] For principle of data minimisation see Article 5(1)(c), GDPR.

[288] See in particular Article 5(1)(f) and Article 32, GDPR.

[289] See in particular Articles 5(2) and 24(1), GDPR.

[290] DPA's Opinion on Draft Law Draft law for a Federal Act amending the E-Government Act and the Passport Act 1992 (Implementation E-ID), (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 02 October 2020).

Act 2000 and the Research Organisation Act[291], the Austrian DPA needed to comment on data transmission via an "interface for electronic data exchange". After explaining that such a requirement is not based on the GDPR, the DPA explained that more detailed requirements on the quality of such an interface need to be laid down in national regulation in order to define these interfaces in a uniform manner and, on the other hand, to ensure that they correspond to the respective state of the art safeguards (e.g., ÖNORM, ISO standard).

The Spanish DPA also establishes a similar position that the transmission of data requires specific national provisions. Already in 2013, the **Spanish Constitutional Court**[292] held that although administrative law creates a general principle of inter-administrative collaboration, any data transmission between public authorities needs to be done in accordance with Spanish data protection law. In its decision on the Balearic Islands' Office for the Prevention of Corruption's use of COVID-19 vaccination data[293], the **Spanish DPA** decided that the legal instrument required to enable the use of data collected for one purpose by the Health Service was not justified as it lacked sufficiently transparent information on the specific purpose for which the data was required. The AEPD referred in particular to CJEU case law in order to discuss the requirement for transparency and foreseeability in legislation enabling widespread interference with individual rights[294]. In a recent opinion on a consultation raised by the National Competition Authority (CNMC) on the possibility of providing the National Statistical Centre a sample of phone numbers of women[295], the AEPD authorised the CNMC to provide a sample but under certain conditions[296]. The Spanish DPA said that one public authority may transmit data (phone numbers) to other authorities for the purpose of a survey if **specific national legislation provides for such a legal obligation**. However, the transmission of such personal data should be subject to data protection principles in Article 5 GDPR, which firstly requires an analysis of whether intended communication is proportional to the intended purpose. Communication of data from one public authority to the other is only lawful if **appropriate safeguards** are put in place (e.g., separation of special categories of personal data from other data, consent in case of processing of special categories of personal data, short retention periods) and if this is **strictly necessary** in all circumstances[297]. In case the use of data from administrative sources is required for mandatory statistical purposes, the AEPD seems less strict in its assessment of further use[298]. Data communicated from one public authority to another for a certain purpose, can under no circumstances be reused for an additional purpose[299].

A **Romanian** case[300] explains that transmitting data between national authorities (in the case of state tax authorities and other bodies) is lawful if based on specific national legal provisions. The Court said that the case is not about the transmission and processing of data between different institutions, but about the processing and use of data collected by

[291] DPA's Opinion on the draft Federal Act amending the Federal Statistics Act 2000 and the Research Organisation Act, GZ: D055.518 2021-0.474.423 (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 03 August 2021).

[292] Judgment 17/2013 of 31 January 2012, BOE [Official Gazette] number 49, of 26 February 2013 (Constiutional Court).

[293] Procedimiento Nº 0032/2021, (2021c).

[294] Ibid., pp. 30-35.

[295] National Statistical Centre needed the phone numbers in order to conduct the EU Survey on Violence Against Women. As due to pandemic in-person conduction of survey was impossible, the survey needed to be conducted by phone.

[296] Procedimiento Nº: 0060/2021, (2021f).

[297] Ibid.

[298] The AEPD for instance held that when data is required for the production of statistics, the responsible public bodies shall provide the fastest and most expeditious collaboration to the statistical services. See for example: ibid. and Procedimiento Nº 0049/2020 (2020b). . Moreover, further use of phone numbers for mandatory statistics was allowed. See: Procedimiento Nº 0029/2021, (2021b). and Procedimiento Nº 0078/2020, (2021e).

[299] See for example: Procedimiento Nº 0075/2020, (2021d).

[300] Decision no. 2216 of 02 June 2020, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

tax authorities and its territorial units, which are authorised under national law to hold and obtain personal data for the purpose of performing their functions.

Stakeholder interviews provide a further insight into the national legal requirements needed to transmit data between national public bodies.

Box 15: Examples from the stakeholder interviews – Transmission of data

In Romania, interviews revealed that to access the data, public bodies need to comply with the following requirements: (i) be an authorised institution that can process such personal data; (ii) have a clear legal provision (legal basis) authorising them to access such data; (iii) have a clear protocol in place between the institution that provides the administrative data and the institution that requests access; and (iv) clearly define the persons that have the right to use such data.

An interview with a Spanish evaluator revealed that agreements concluded between national authorities and evaluators which are private consultancies help facilitate the transmission of data.

Box 16: Key findings – Transmission of data

- Data transmission in the context of this study is understood as exchanging data between different national actors responsible for ESF+ monitoring or evaluations (i.e., sending or forwarding data on one hand and receiving or accessing data on the other hand).
- Transmission of data falls under the definition of a processing operation, which pursuant to Article 4(2) of the GDPR means any operation or a set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. As any processing of personal data should be lawful, both the access to personal data as well as the receipt of personal data should be based on one of the legal bases in Article 6(1) and be allowed under Article 9(2) in case of transmission of special categories of personal data.
- Transmitting data from one entity to another should also comply with all other basic data protection principles in Article 5 GDPR such as the principle of fairness and transparency, principle of purpose limitation, the principle of data minimisation, the principle of accuracy, and the principle of integrity and confidentiality of personal data.
- Desk research and stakeholder interviews show that the transmission of data is governed by further EU and national legislation and that in order to conclude on the individual obligations of actors involved in transmissions of data for ESF+ purposes, specific national legislation needs to be considered.

5.6. Data linking

For the purpose of this study, ‘data linking’ stands for an operation of database linkage, which is a process of **joining information or data about an individual from different**

databases. Although the GDPR does not use this term, 'data linking' falls under the GDPR definition of 'processing' of personal data[301]. A review of EU-level ESF+ legal framework did not reveal any further rules on data linking.

The linking of data is central to the ability of managing authorities and ESF+ monitoring and evaluation teams to perform their obligations under the ESF+ framework in the most efficient way and without relying solely on participants' data. However, it also presents complex data protection challenges, particularly where the use of data relating to individuals not involved in ESF+ programmes is concerned. The Counterfactual Guidelines stress repeatedly that the use of administrative data is vital to the ability to properly assess the benefits of ESF+ programmes, and that the 'Gap in data' observed during some of the case studies was "the biggest challenge faced by the evaluators".

As in the case of data transmission, any data linking should have a clear legal basis and should comply with data protection principles and rules in the GDPR and the national GDPR-implementing laws[302].

Similarly, national GDPR-implementing laws in the three Member States selected for the in-depth review do not touch upon the issue of data linking. The issue of combining data from different national administrative registers could possibly be addressed in national sectorial legislation in the area of administrative law and will be checked for the purpose of Task 3 in the Final Report. For this reasons, national case law and decisions of national DPAs mostly evolve around the issue of accessing personal data in administrative databases and have already been analysed in other sections of this report (see in particular Section 5.5).

Stakeholder interviews provide an insight into the legal requirements to access statistical data collected by national statistical institutes.

Box 17: Examples from the stakeholder interviews – Linking of statistical data

The Spanish Statistical Institute (Eustat) mentioned that processing statistical data in Spain is strictly regulated. While public statistical institutes have access to multiple types of data from different sources, they are not allowed to use or share them due to data protection and statistical secrecy rules.

Similar restrictions apparently exist in Romania, where the national Institute of Statistics is not allowed to share any administrative data.

Box 18: Key findings – Data linking

- 'Data linking' stands for an operation of database linkage, which is a process of joining information or data about an individual from different databases. Although the GDPR does not use this term, 'data linking' is considered a processing operation and hence requires a clear legal basis and compliance with other GDPR requirements.

[301] See Article 4(2), GDPR.

[302] Linking is also closely related to the notion of further processing which is discussed in depth in Section 0 above.

- No rules addressing the issue of data linkage for ESF+ monitoring and evaluation purposes could be found in the EU or national data protection legislation of the three Member States selected for in-depth analysis.

5.7. Data storage

After explaining the rules on data retention in the EU and national data protection (Sub-section 5.7.1), this Section analyses the legal obligations arising from the EU law when storing individual level administrative data for evaluations or monitoring, supplemented with examples of national legal obligations and practices in Austria, Romania, and Spain (Sub-section 5.7.2).

5.7.1. Rules on data retention

Rules on data retention are based on one of the key data protection principles under Article 5 GDPR - storage limitation[303]. This principle implies that data should be kept in a form which permits identification of data subjects for **no longer than necessary** for the purposes for which the personal data are processed (e.g., principle of data minimisation). As a rule, the data retention periods should be based on the necessity of the data storage for the purpose for which the personal data are being processed.

An **exception** to this rule only applies when processing for archiving purposes in the public interest, **scientific** or historical **research purposes or statistical purposes** in accordance with Article 89(1) GDPR. In such cases personal data may be stored for longer periods, subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subjects[304].

National GDPR-implementing laws and other (sectorial) laws can provide for processing-specific retention periods, albeit in line with the principle of data minimisation. At Member State law level, in Austria, DSG cross-refers to the GDPR with respect to storage limitation principle and does not provide any rules on retention of data. The same is true for Spain. **Romanian** data protection law, however, mentions retention periods in two scenarios: firstly, as one of the appropriate safeguards for processing of (special categories of) personal data for (substantial) public interest[305]; and secondly, when it sets a specific retention period for the processing of data through electronic monitoring and/or video surveillance systems at the workplace[306].

5.7.2. Legal obligations arising from the EU and national laws

The GDPR provides for a general framework for the protection of personal data, meaning that it does not set precise rules for every processing operation. With respect to data retention, **Article 5(1)(e) GDPR** incorporates the principle of storage limitation. **Article 25(2) GDPR** is also relevant in this respect as it sets the requirements to **data protection by default**. It requires the controllers to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each

[303] Article 5(1)(e), GDPR.

[304] Idem.

[305] See for example Article 4(2)(c) and Article 6(c) Law no. 190/2018.

[306] Article 5(e) Law no. 190/2018.

specific purpose of the processing are processed. The obligation of 'data protection by default' hence also refers to the choices made by the controller that have an effect on the data retention period[307]. If personal data are no longer necessary for the purpose of the processing, they should be deleted or anonymised by default [308].

As a result, storage periods should be set by Union or national legislation and/or determined by controllers with respect to every processing operation.

Concerning ESF+, a precise retention period is set in **Article 82(1) CPR 2021**, which states that the managing authorities shall ensure that all supporting documents related to an operation supported by the Funds (i.e., the ESF+) should be kept for **a five-year period, from 31 December of the year of the last payment by the managing authority to the beneficiary**[309]. When commenting on a similar provision in Article 90 of the Regulation 1083/2006, the EDPS stated that if data are kept in accordance with the prescribed storage period, it has no reason to believe that personal data are kept in a form which permits identification of data of data subjects for longer than is necessary[310]. The EDPS has nonetheless recommended including a respective obligation for a data controller to delete personal data after the end of the retention period in writing[311].

Data intended for ESF+ monitoring or evaluations need to be hence stored **for five years** from 31 December of the year of the last payment by the managing authority to the beneficiary before they can be deleted. This period indicates the **specific duration** for which data can be stored for ESF+ monitoring and evaluation purposes.

National DPAs often comment on the principle of storage limitation. For example, when reviewing draft Government Emergency Ordinance granting parents free days to supervise their children during the pandemic, the Romanian DPA said that national legislation providing for the processing of data must include clear provisions also on the retention of data, in particular where children's data are concerned[312]. When commenting on an Act amending the Epidemic and COVID-19 Measures Act, the Austrian DPA stated that the retention of personal data beyond the period set out in the legislation is not permissible[313].

Concerning the issue of **whether the managing authorities are obliged to delete the ESF+ participants' monitoring data (or part of it) if the participants ask to do so,** the answer depends on several factors, such as the legal basis for processing. The right to erasure of personal data is not absolute and applies in one of the following situations: (i) data are no longer necessary in relation to the purpose for which they were collected or otherwise processed; (ii) **consent is withdrawn** and no other legal basis exists; (iii) the **data subject objects to the processing** pursuant to Article 21(1) GDPR and there are no

[307] European Data Protection Board. (2020b). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. para. 41. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[308] Ibid.para. 53.

[309] Article 82(1), CPR 2021.

[310] European Data Protection Supervisor. (2014). *Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the "Risk analysis for fraud prevention and detection in the management of ESF and ERDF" - ARACHNE*. https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check/risk-analysis-fraud-prevention-and_en, p. 10.

[311] Ibid.

[312] Review of draft Government Emergency Ordinance on granting free days to parents for the supervision of children, in the event of the suspension of courses or the temporary closure of some educational establishments due to the spread of the coronavirus SARS — COV-2. (Gov Emergency Ordinance 147/2020), 24 September 2020, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro.

[313] Opinion of the Data Protection Authority on the draft assessment of the Federal Act amending the 1950 Epidemia Act and the COVID-19 Measures Act, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 5 March 2021). https://www.parlament.gv.at/PAKT/BEST/SN/index.shtml, p. 2.

overriding legitimate legal bases for processing (such as public interest); (iv) personal data have been processed unlawfully; (v) personal data have to be erased to comply with a legal obligation in Union or Member State law to which the controller is subject; or (vi) personal data have been collected in relation to the offer of information society services referred to in Article 8(1)[314]. Upon such a request, the controller is without undue delay obliged to stop with all processing operations (including storage of data) and needs to delete all data about such participants[315]. For instance, if the processing of ESF+ participant's monitoring data was based on consent, a withdrawal of a consent logically results in the prohibition to further process participant's data as the legal basis has been removed[316]. As mentioned, **the right to erasure is not absolute** and can be rebutted, if the processing is still necessary, for one of the following cases: (i) for exercising the right of freedom of expression and information; (ii) for compliance with a legal obligation that requires processing by Union or Member State law to which the controller is subject or the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; (iii) for reasons of public interest in the area of public health; (iv) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) if the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (v) for the establishment, exercise or defence of legal claims[317]. In the context of ESF+ monitoring and evaluation in particular exemptions in Article 17(3)(b) – compliance with a legal obligation or task in public interest are relevant when the processing is based on Union or Member State law. Any exception to the exercise of data subjects' rights should be narrowly construed.

Box 19: Key findings – Data storage

- The storage limitation principle (Article 5(1)(e) GDPR) requires that data should be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed.
- Storage periods are set either by Union or national legislation and/or determined by controllers with respect to every processing operation. If personal data are no longer necessary for the purpose of the processing, then the controller should delete or anonymise them by default.
- Based on Article 82(1) CPR 2021, data intended for ESF+ monitoring or evaluations need to be stored for auditing purposes for five years from 31 December of the year of the last payment by the managing authority to the beneficiary before they can be deleted. When managing authorities are obliged to delete the ESF+ participants' personal data depends on the legal basis for such processing as the right to erasure of personal data is not absolute.

[314] Article 17(1) GDPR.

[315] In fact, the controller who made such data public even needs to take reasonable steps to inform other controllers which are processing such personal data that the data subject has requested the erasure. See Article 17(2), GDPR.

[316] Article 7(3), GDPR. Note that the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

[317] Article 17(3), GDPR.

5.8. Informing data subjects

In this Section the transparency obligations of the controller stipulated in Articles 12 (transparency), 13 (information obligation where data are obtained from the data subject) and 14 GDPR (information obligation where data are not obtained from the data subject) are discussed (Sub-section 5.8.1). Finally, the conditions and practical implications of transparency obligation for the monitoring and evaluation of the ESF+ are discussed in Sub-section 5.8.2.

5.8.1. Information obligation

Obligation of informing data subjects is an expression of the **principle of transparency**. Within the context of the GDPR, transparency is an overarching obligation applying to three central areas: (i) the provision of information to data subjects about the processing of their personal data as an expression of fairness of that processing[318]; (ii) how data controllers communicate with data subjects in relation to their data protection rights; and (iii) how data controllers facilitate the exercise by data subjects of their rights[319].

The concept of transparency in the GDPR is user-centric rather than legalistic. The objective is to make data subjects understand in non-technical language what is happening with their data and what rights they have. While transparency is not defined in the GDPR, recital 39 provides some information on the meaning and the effect of the principle.

The rules concerning the information obligation of the controller are outlined in Articles 12 – 14 GDPR. Article 12 sets out the general rules on the provision of information to data subjects which apply inter alia where data are obtained from the data subject (Article 13) and where data are obtained from other sources and not the data subject (Article 14).

Article 12 requires that any provision of information and communication with data subjects should be done in a concise and transparent manner (e.g., usage of layered or staggered privacy statements), the information provided should be intelligible (e.g. understandable by an average person) and in an easily accessible form (e.g. privacy statement should be clearly visible on each website), using clear and plain language (e.g. not too legalistic). Information should be provided in writing or by other means such as electronically or even orally (if requested by the data subject). The provision of information should be free of charge for the data subject. Special care is needed in case of provision of information to children and other vulnerable individuals[320].

Transparency requirements in the GDPR **apply irrespective of the legal basis** for processing and throughout the life cycle of processing[321]. This means that the controller needs to inform data subjects about the processing of their data also when the legal basis is other than consent, unless exception to information obligation could be established.

[318] Principle of fairness is about engendering trust in the process by enabling data subjects to understand the processing of their data and to be able to exercise their rights in case of unlawful processing.

[319] Article 29, Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/622227/en.

[320] Ibid., paras. 14-16.

[321] Ibid., para. 5. Article 12 GDPR makes it clear that that transparency applies in all stages of the data processing cycle (e.g. before the start of the processing – i.e. when personal data are collected from the data subjects or other sources; throughout the processing period – i.e. when communicating with data subjects about their rights; and at specific points like in case of data breaches).

In line with Articles 13 and 14, a controller needs to provide the data subjects with the following information[322]:

- the identity and the contact details of the controller, and where applicable their representative;
- contact details of the DPO;
- the purpose(s)[323] and legal basis for the processing[324];
- the legitimate interests pursued in cases where "legitimate interests" is the legal basis[325];
- categories of personal data concerned[326];
- recipients or categories of recipients of personal data (e.g. other controllers, joint controllers, processors or other third parties to whom the data is transmitted or disclosed);
- details of transfers to third countries outside EU/EEA legal space and the corresponding mechanism;
- retention periods, or, if not possible, criteria used to determine such periods;
- the rights of the data subjects[327];
- where processing is based on (explicit) consent, the right to withdraw consent at any time;
- the right to lodge a complaint with a DPA;
- where processing is based on a contract, the possible consequences of failure[328];
- in case the data are not obtained from the data subject, the source from which the personal data originate and if applicable if it came from a publicly accessible source;

[322] WP 29's position is that there is no difference between the status of information provided under Paragraphs 1 and 2 of Articles 13 and 14 and that all information is of equal importance. See ibid., para. 23. See Article 13(1) and (2) as well as Article 14(1) and (2).

[323] If the purpose includes the creation of inferred personal data, the intended purpose of creating and further processing such inferred personal data, as well as the categories of the inferred data processed, must always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose in compliance with Articles 13(3) or 14(4). See ibid., p. 14. However, if the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided instead. See recital 61, GDPR.

[324] In case of processing of special categories of personal data, also the relevant exemptions from Article 9(2) (and where relevant the applicable Union or Member State law under which the data is processed) on top of a legal basis from Article 6(1) should be specified.

[325] As legitimate interest in Article 6(1)(f) GDPR cannot be a valid legal basis for public authorities, provision of this information is obsolete in case of processing of personal data by public bodies.

[326] This information is only required in case personal data have not been obtained from data subjects, as they lack an awareness of the types of data the controller has obtained about them.

[327]It is not necessary that the data subjects have at their disposal all rights as stipulated in Articles 15-22 GDPR as the scope of the rights might also depend on the legal basis of processing.

[328] Similar as in case of legal interest, the legal basis in Article 6(1)(b) – processing is necessary for the preparation or performance of a contract to which the data subject is a party – is an unsuitable legal basis for processing data in the scope of ESF+ monitoring or evaluation.

- the existence of automated decision-making, including profiling and if applicable meaningful information about the logic used and the significance and envisaged consequences on a data subject.

Pursuant to Articles 13(3) and 14(4), GDPR controllers are also obliged to **include information about the planned further processing** (e.g., transmission of data for an additional purpose). If the circumstances of such a secondary use of data are already known at the moment of the data collection, the information provided to data subjects should also cover details of such further processing. If further processing and its modality is, however, not yet known at the time of data collection, the information could be provided later, but in any case, **prior to that further processing**[329]. Information about the planned further processing needs to include, in particular, the **purpose for such further processing or reuse of data** as well as any other relevant further information as stated in Articles 13(2) or 14(3) GDPR, such as the details on the recipients or the categories of recipients of the processed personal data. The term recipient is defined in Article 4(9) GDPR and the opinion of the EDPB includes data protection actors (e.g., other data controllers, joint controllers, processors) or any other third-party recipients[330].

The above specified information should be provided to the data subjects at the commencement phase of the processing cycle. The issue of timing is a vital element of the transparency requirements and is inherently linked to the concept of fair processing. If the personal data are collected from the data subjects, the controller should inform them **at the time when personal data are obtained** (Article 13(1) GDPR). If the data are not obtained from the data subject, the controller should inform them within a reasonable time after obtaining the personal data, but at the latest within one month or if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication (Article 14(3) GDPR).

Several **exceptions** to the obligation to provide information exist both in the case of Article 13 and Article 14 GDPR. If a controller can demonstrate the existence of an exception, he or she is relieved from the information obligation. However, any exception to the transparency obligations should be **interpreted and applied in a restricted way**.

If data are collected directly from the data subjects, the only possible exception is if a data subject already has the information[331]. Article 14(5) GDPR provides for a broader set of exceptions to the information obligations, and includes the following four situations:

- when a data subject already has the information[332];

- when the provision of information proves impossible (e.g., the controller does not have contact details of data subjects) or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or would render impossible or

[329] See in particular Articles 13(3) and 14(4), GDPR. These Articles specify that in case of processing of data for a further purpose, the controller should provide to data subjects any relevant information with respect to such further processing. In the opinion of the WP29 and in line with recital 61, the controller does not have any leeway and should provide to data subject all information as requested in Articles 13 or 14, unless one or more categories of the information does not exist or is not applicable. See Article 29, Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/622227/en, para. 46.

[330] Ibid., p. 37. In accordance with the principle of fairness, controllers must provide data subjects with information that is most meaningful for them (e.g. the actual names of the recipients, or in case of categories of recipients a specific reference to the activities they carry out, the industry, sector and sub-sector they belong to and their location).

[331] Article 13(4), GDPR.

[332] Article 14(5)(a), GDPR.

seriously impair the achievement of that processing (e.g., money laundering investigations)[333];

- when obtaining or disclosure is expressly laid down by EU or national law (e.g., a tax authority is subject to a mandatory requirement under national law to obtain the details of employees' salaries from their employers) and such a law provides appropriate protection for the data subject's legitimate interests[334]; or

- where personal data must remain confidential subject to an obligation of professional secrecy (e.g., medical secrecy)[335].

A review of national GDPR-implementing laws revealed that while Austrian and Romanian data protection laws do not provide any rules on provision of information, **Spanish** law differentiates between certain "basic" information listed in Articles 13 and 14 GDPR that need to always be provided to the data subject and some information listed in these Articles that could also be provided through electronic means that allow easy and immediate access to them[336].

5.8.2. Legal obligations arising from the EU and national laws for processing data for ESF+ monitoring or evaluation

For evaluation of ESF+ programmes, evaluators often need to access existing administrative data from different public databases. Data subjects whose data are contained in such databases were at the time of data collection most likely not informed about the potential use of their data for ESF+ evaluation purposes. The question arises **if and how to inform such data subjects that their data is being processed for an additional purpose (i.e., ESF+ evaluation)**[337]. As explained above, the principle of transparency applies throughout the processing life cycle. The controller needs to adhere to the same principles when communicating both the initial information and any subsequent substantive or material changes, such as the change of processing purpose[338]. The WP29 further recommends that the privacy notice also explains how the processing for the new purpose is compatible with the original purpose[339]. If an organisation collecting personal data (e.g., beneficiary) maintains a website, a privacy statement/notice should be also published on the website so that it is clearly visible on each page under a commonly used term. Article 46 CPR 2021 instructs Member States to set up and maintain a single website portal providing access to all programmes involving that Member State[340]. Although the aim of such national portals is to communicate to Union citizens the role and achievements of the Funds, the website could also be used as a tool to inform data subjects about processing of their personal data. Note that **informing data subjects solely through a website might not be sufficient**. In its ARACHNE Opinion the EDPS held that the publication of the Privacy Statement on the Europa Social Fund website does not in itself suffice to ensure that data subjects effectively receive the information, as not all possible data subjects will

[333] Article 14(5)(b), GDPR.

[334] Article 14(5)(c), GDPR.

[335] Article 14(5)(d), GDPR.

[336] Article 11, Organic Law 3/2018.

[337] It must be noted that the compliance with transparency requirements does not release a controller from complying with other rules in the GDPR, including the principle of purpose limitation as explained in Section 0.

[338] Article 29, Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/622227/en, para. 29.

[339] Ibid., para. 47.

[340] Article 46(b), CPR 2021.

read the information published on the website[341]. The EDPS therefore considered that this publication must be complemented, to the extent possible, by some form of individual information[342]. For instance, when data are collected directly from participants, all necessary information should also be provided at this point in time.

What is not clear from the text of the GDPR is **when precisely changes to information should be notified to the data subjects**. When deciding whether data subjects should be informed about the use of their personal data also for the monitoring and evaluation of the ESF+, the controller must have regard to the principles of fairness and accountability. Any fundamental change to the nature of the processing (such as a transmission of data for evaluation purposes) should be brought to data subjects' attention well in advance[343] and should include an explanation on the likely impact of those changes on data subjects[344]. Any information in relation to further processing must be provided **prior to that further processing** and a reasonable period should occur between the notification and the commencement of processing so that the data subjects have a meaningful opportunity to consider such further processing and potentially exercise their rights in relation to this. In line with the principle of fairness, more intrusive processing operations require a longer period[345]. Where data were at least partially previously collected from data subjects themselves, the EDPS in its ARACHNE Opinion recommended providing necessary information at the point when data is obtained from the ESF and ERDF managing authorities (through the SFC2007 infrastructure)[346]. By analogy, data subjects should be informed about the reuse of their personal data prior to the moment when data are collected from them and at the point where further data concerning them are obtained from administrative authorities.

The **GDPR does not prescribe an exact wording/template of an information notice**. The controller is responsible to take "appropriate measures", which means it should take into account all of the circumstances of the data collection and processing when deciding upon the appropriate modality and format by which information should be provided to data subjects. Guidelines, opinions and other similar documents of the EU data protection bodies (i.e., WP29, EDPB, EDPS) and national DPAs provide further guidance. For instance, the WP29 recommends that an organisation collecting personal data (e.g., beneficiary) that maintains a website, publishes a privacy statement/notice on its website so that it is clearly visible on each page under a commonly used term[347]. The controller is obliged to take active steps to provide the data subjects with all information in one single place or document[348].

Finally, the Technical Specifications[349] also pose the question **how data subjects could be informed in practice** if the data are very large and cover a longer time span. Whilst the text above already discusses the option to inform data subjects via a website, this Section

[341] European Data Protection Supervisor. (2014). *Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the "Risk analysis for fraud prevention and detection in the management of ESF and ERDF" - ARACHNE*. https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check/risk-analysis-fraud-prevention-and_en, p. 12.

[342] Ibid.

[343] Article 29, Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/622227/en, para. 30.

[344] Ibid., para. 31.

[345] Ibid., para. 48.

[346] European Data Protection Supervisor. (2014). *Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the "Risk analysis for fraud prevention and detection in the management of ESF and ERDF" - ARACHNE*. https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check/risk-analysis-fraud-prevention-and_en, p. 12.

[347] Article 29, Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/622227/en, paras. 11 and 24.

[348] Ibid., para. 33. The principle of accountability also requires controllers to be able to explain and demonstrate how the tool/approach chosen to convey the information is the most appropriate in their case.

[349] Technical Specification, p. 13.

further describes **situations where the controller is exempt from its obligation to inform data subjects**.

Firstly, as discussed in Sub-section 5.8.1, four **exemptions** apply when data were not obtained from the data subject (Article 14(5) letters (a)–(d)), which should, however, be interpreted and applied narrowly[350]. Letters (b) and (c) are particularly relevant for informing data subjects in the framework of ESF+ monitoring and evaluation and are thus discussed.

Article 14(5)(b) GDPR, for example, allows for three separate situations where the obligation to provide information in Article 14 is lifted: (i) where it proves impossible (in particular for achieving, scientific or historical research or statistical purposes); (ii) where it would involve a disproportionate effort (in particular for achieving, scientific or historical research or statistical purposes); and (iii) where providing the information required would make the achievement of the objectives of the processing impossible or seriously impair them. If the controller would like to rely on the first situation under letter (b) ("**proves impossible**"), factors that actually prevent the provision of information to data subjects would need to be demonstrated (e.g., the controller has no means to directly contact the data subject as it does not have their contact details)[351]. The second exemption under letter (b) relates to situations of **"disproportionate effort"**. Recital 62 provides some indicative issues that contribute to a data controller having to make disproportionate effort such as the number of data subjects, the age of the data and any appropriate safeguards adopted. The WP29's position is that this exception should not be routinely relied upon, and that the disproportionate effort must be directly connected to the fact that the personal data was not obtained from the data subject[352]. The controllers would need to carry out and document a balancing exercise weighing the effort involved in providing information to the data subjects and the impact and effect on the data subjects if they are not provided with the information[353]. One of the issues is how Article 11 GDPR that governs processing that does not require identification, such as obtaining access to pseudonymised information from administrative registers fits with the information obligation in Article 14(5)(b) GDPR. When accessing pseudonymised administrative data from national registers for the purpose of ESF/ESF+ monitoring and evaluation, Article 11 could prevent information being given to the data subject prior to the reuse of administrative data, essentially depriving the data subject of their fundamental right to transparency of processing.

The controller could also rely on exemption in **Article 14(5)(c)**, if the **obtaining or disclosing of personal data is expressly laid down by Union or Member State law to which the controller is subject**. This exemption is conditional upon such law providing appropriate measures to protect the data subject's legitimate interests. The controllers have to ensure and be able to demonstrate that their obtaining or disclosure of data comply with those measures[354].

Review of **case law in Romania** shows that the exemption in Article 14(5)(c) can be relied upon especially in case of public authorities that are processing data in the scope of their investigation activities. On several occasions, the High Court of Cassation and Justice Judgment did not find breaches of data protection law even though public authorities did not inform data subjects about the processing[355]. The Court held that since a special national

[350] Article 29, Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/622227/en, ibid., para. 57.

[351] In the opinion of the WP29, this situation is very rare in practice. See ibid., para. 59.

[352] In the opinion of the WP29, this situation is very rare in practice. See ibid., paras. 61-62.

[353] In the opinion of the WP29, this situation is very rare in practice. See ibid., para. 64.

[354] In the opinion of the WP29, this situation is very rare in practice. See ibid., para. 66.

[355] Decision no. 6460 of 02 December 2020, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)). and Decision no. 2752 of 23 June 2020, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

legislative act was issued (as opposed to an administrative act as it was the case in the *Bara* case), such act ensures that data subjects are informed about the transmission of their data in advance.

Moreover, Article 23 GDPR provides for Union or Member States to legislate for further **restrictions** on the scope of data subjects' rights, including the right to transparency in Articles 12-14 GDPR. Any such restriction needs to respect the essence of the fundamental rights and freedoms and needs to present a necessary and proportionate measure in a democratic society to safeguard one of the ten objectives set out in Article 23(1)(a)-(j)[356]. For such a Union or national provision to be a valid restriction, it needs to meet clear criteria listed in Article 23(2), one of which is also that it needs to contain a provision as to the right of the data subject to be informed about a restriction on their rights[357]. Where such national measures restrict either the specific data subject rights or the general transparency obligations, which would otherwise apply to data controllers under the GDPR, the data controllers should be able to demonstrate how the national provision applies to them and should also inform data subjects that they are relying on such a national legislative restriction to the transparency obligation[358].

Desk research at EU level and national level (limited to national data protection laws of Austria, Romania and Spain) did not reveal such further exemptions that would legitimise non-provision of information.

Box 20: Key findings – Informing data subjects

- Article 12 GDPR requires that any provision of information and communication with data subjects should be done in a concise and transparent manner, the information provided should be intelligible and in an easily accessible form, using clear and plain language. Information should be provided in writing or by other means such as electronically or under certain conditions even orally.
- Transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. This means that the controller needs to inform data subjects about the processing of their data, unless exception to information obligation could be established under Article 13 or Article 14 GDPR.
- Pursuant to Articles 13(3) and 14(4) GDPR controllers are also obliged to include information about the planned further processing or reuse of data (e.g., transmission of data for an additional purpose). Information about the planned further processing needs to include in particular the purpose for such further processing or reuse of data as well as any other relevant information as stated in Articles 13(2) or 14(3) GDPR.
- In case of data processing for ESF+ monitoring and evaluation purposes stakeholders should think of informing data subjects about the processing of their data not only through a website but also through other means, especially when

[356] Such objectives for example include: important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security (Article 23(1)(e)); a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g) (Article 23(1)(h)); or the protection of the data subject or the rights and freedoms of others (Article 23(1)(i)).

[357] Article 23(2)(h), GDPR.

[358] Article 29, Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/622227/en, para. 68.

personal data are collected directly from participants. In principle, data subjects should be provided with all information in one single place or document.

- Where personal data have not been obtained from the data subjects (non-participants) they do not need to be informed about the processing of their data, if the controller can prove the existence of an exception in Article 14(5) of the GDPR. Letters (b) and (c) of Article 14(5) of the GDPR are relevant as they could exempt the controller from an information obligation in case such action proves impossible or would entail a disproportionate effort. An exemption according to these provisions is also possible in case obtaining or disclosing data is expressed in Union or Member State law, providing appropriate measures to protect the data subject's legitimate interests.

6. Conditions to access data and models of data access

This Section provides an overview of the different models used for accessing administrative data both for ESF/ESF+ monitoring and evaluation purposes (Section 6.1) and the legal implications of each of these models (Section 6.2). After providing a brief practical description of the different models for using administrative data in all nine Member States covered by this study, the systems for accessing and using administrative data in Austria, Spain and Italy are analysed in more detail. The countries selected for in-depth analysis were carefully chosen so that the final selection included at least one decentralised country (Spain).

6.1. Models in accessing administrative data

This Section begins with a description of two different models of access to administrative data observed – centralised and decentralised, and which Member State belongs to each model. Thereafter, a brief description is included of each Member State's model for accessing administrative data for ESF/ESF+ monitoring and evaluation, followed by a more in-depth analysis of the models in three Member States - Austria, Spain, and Italy.

6.1.1. Different types of models

Based on interviews and desk research, most country models to access and link administrative data for ESF/ESF+ monitoring and evaluation are decentralised across different institutions and levels of government. **Sweden** is the only Member State out of the nine covered in this study that has centralised its model of access to administrative data for ESF/ESF+ monitoring and evaluation. The model of access to administrative data in Sweden could be described as **centralised and harmonised** as all data processing and linking is centralised to Statistics Sweden. Models of access to administrative data in all **eight** other **Member States** (Austria, Germany, Spain, France, Ireland, Italy, Poland, and Romania) are **decentralised**. In these Member States, there may be central databases that store data that are collected directly from the ESF/ESF+ participants and the managing authorities may play a certain coordinating role. However pre-existing administrative data that are used to complement and link data for monitoring and evaluation are neither coordinated nor processed centrally. Moreover, evaluators can also access administrative data without the need to inform the managing authority. For example, in Spain, France,

Poland, and Romania, administrative data must be accessed from each individual institution that hosts these data, and the processes to do so may vary depending on the institution and region. In Ireland, there are attempts to harmonise datasets such as via the JLD, and there are examples of coherent models used by individual intermediary bodies with access to their own administrative data. However, there is no nation-wide model, and the managing authority is not involved in the process. Lastly, whilst the Austrian managing authority manages a central database containing participants data collected for ESF/ESF+ purposes, access to administrative data for ESF/ESF+ purposes is not centralised nor harmonised.

Austria: In Austria, a central database containing data that are collected directly from the ESF/ESF+ participants exists and the managing authority plays a coordinated role. However, there is no single institution that the managing authority has contracted to jointly host and link administrative data for ESF/ESF+ purposes as is the case in Sweden. There is still limited experience in accessing administrative data for evaluation purposes, but in principle intermediary bodies or other evaluators can access administrative data for ESF/ESF+ evaluation purposes without the involvement of the managing authority. More information on the Austrian model is in Section 0 below.

Germany: In Germany, there are several previous examples of centrally managed processes for linking administrative data. For, example, the Integrated Employment Biographies (IEB) have integrated administrative data sources of the Federal Employment Agency[359]. Moreover, the Federal Employment Agency is responsible for linking unemployment register data with several other datasets[360]. However, linking administrative data from the unemployment register to other data sources such as surveys is not possible in Germany due to the lack of unique identifiers[361] and possibly due to legal restrictions that require informed consent from survey respondents[362]. In an ESF context, a study from 2018 reported a limited use of administrative data for ESF monitoring purposes, partly due to the lack of data availability and data protection restrictions. However, the study found one example of the use of administrative data for ESF evaluation purposes, by the OP Niedersachsen ESF/ERDF[363]. This study has, via interviews, identified one regional managing authority that has used administrative data for ESF monitoring, and one evaluator that was contracted one time to use administrative data for an evaluation for the federal managing authority. Data in all examples have been anonymised, and several interview respondents have expressed challenges to access administrative data. Based on information gained from two managing authorities interviewed, one national and one regional, administrative data are stored at three levels of government: federal, regional, and local levels. According to these interviewees, there are only two central administrative datasets, which are held by the Employment Agency and the Central register for foreigners. Also, many datasets are only stored within individual institutions such as schools, and these may not be comparable. The ESF/ESF+ managing authorities are not allowed to access these due to data protection reasons. Only research institutes and selected authorities may do so. Thus, although there are previous examples in the literature of central systems for linking administrative data, there are currently no examples of systematic or centrally managed systems in a German ESF context.

Spain: As Spain is a decentralised country, it is logically also an example of a decentralised model of access to administrative data. Several examples of the use of administrative data, for both ESF monitoring and evaluation were identified during the interviews. More

[359] European Commission. (2021). *Design and commissioning of counterfactual impact evaluations : a practical guidance for ESF managing authorities*. https://data.europa.eu/doi/10.2767/02762, p. 37.

[360] OECD. (2020). *Impact evaluation of labour market policies through the use of linked administrative data*. https://www.oecd.org/els/emp/Impact_evaluation_of_LMP.pdf , p. 49.

[361] Ibid., p.61.

[362] Ibid., p.63.

[363] European Commission. (2018b). *Study on the monitoring and evaluation systems of the ESF: Final report*. Annex 13: Country Report – Germany.

information on the Spanish model of access to administrative data is provided in Section 6.1.3.

France: Among the nine Member States in this study, France was the only country with an ESF specific identifier code for the ESF monitoring system, according to a study from 2019[364]. However, difficulties arose regarding the comparability of administrative data[365]. From the interviews in this study, there were examples of the use of administrative data for both monitoring and evaluation. Data are accessed both from national databases and regional databases, and persons that can access these data vary from institution to institution holding the data.

Ireland: While there are examples in Ireland of the use of unique identifiers (pseudonymised IDs) in the ESF monitoring system that can be linked to other administrative data concerning the labour market[366], an OECD study states that survey data and administrative data from the main unemployment register cannot be linked due to the lack of common unique identifiers[367]. Both for monitoring and evaluation of the ESF, challenges have previously been observed regarding inconsistent information between administrative data and ESF indicators[368]. There are several difficulties observed in this study. According to interviewees in this study, administrative data for ESF monitoring and evaluation is used, but can only be accessed either by the individual institution hosting the data, or via the JLD. The JLD can link administrative datasets and have been used on several occasions to evaluate ESF programmes by contracted evaluators, who access pseudonymised data to carry out their evaluations[369]. Information received from interviewees in this study describes that this dataset draws together payment and administrative data from the Department of Social Protection and data from SOLAS and the Revenue Commissioners. However, ESF intermediary bodies interviewed mainly use data from their own registers for evaluation purposes, and the national managing authority is not directly involved in the process. In a follow-up consultation with the Department of Social Protection, a stakeholder stated that they process personal data as original controller for the purposes of claim processing, income support and employment services. Data which are collected for specified, explicit and legitimate purposes is further processed in accordance with Article 89(1) of GDPR, for scientific research and statistical purposes, practices which are not incompatible with the initial basis for data collection. Regarding the JLD, researchers have previously had access to an extract of the database in circumstances where they are trying to answer a policy question of interest to the Department. This access was subject to a data sharing agreement[370].

Italy: In Italy, the model of access to administrative data for ESF purposes is decentralised both between institutions and between levels of government. The systems for accessing administrative data are not integrated, and the access to administrative data is managed by each region as described in Section 6.1.4. It is worth remembering that Italy is a decentralised country with 21 ESF regional managing authorities (21 regional operational programmes) and some ESF national managing authorities (8 national operational

[364] European Commission. (2019b). *Pilot and feasibility study on the sustainability and effectiveness of results for European Social Fund participants using counterfactual impact evaluations: Final report*. p. 68.

[365] European Commission. (2018b). *Study on the monitoring and evaluation systems of the ESF: Final report*. Annex 13: Country Report – France.

[366] European Commission. (2019b). *Pilot and feasibility study on the sustainability and effectiveness of results for European Social Fund participants using counterfactual impact evaluations: Final report*. p. 69.

[367] OECD. (2020). *Impact evaluation of labour market policies through the use of linked administrative data*. https://www.oecd.org/els/emp/Impact_evaluation_of_LMP.pdf , p. 61.

[368] European Commission. (2018b). *Study on the monitoring and evaluation systems of the ESF: Final report*. Annex 13: Country Report – Ireland.

[369] European Commission. (2021). *Design and commissioning of counterfactual impact evaluations : a practical guidance for ESF managing authorities*. https://data.europa.eu/doi/10.2767/02762, p. 39.

[370] Consultation of the Department of Social Protection, 13 June 2023.

programmes)[371]. In order to monitor the financial and physical implementation of the programmes co-financed by ESIF at the national level, the Ministry of economy (MEF-IGRUE) has set up a centralised National Monitoring System (BDU), which is fed by the regional information systems on the basis of a common data record shared with the regions. This data set stores information on both beneficiaries and entities and financial quantities and can be accessed for monitoring and (partially) evaluation purposes by authorised subjects[372].

Poland: A study from 2019 reported that there are separate channels to access administrative data for ESF purposes. At regional level, access is agreed with the local Public Employment Service that administers the database Syriusz, and access at a central level is agreed with the Ministry of Labour[373]. In addition, administrative data from the Public Employment Service do not include employment status data, which may require other means of data collection[374]. A consultation with one ESF operational programme managing authority concluded that administrative registers are not used to collect data for ESF indicators because of inconsistencies between variables[375]. Considering interview answers in this study, the processing of administrative data is not fully centralised in Poland. While the transmission and storage of participants' personal data are harmonised within the country, different administrative datasets have been used and the ways to access these have differed depending on the actor. Moreover, administrative data are stored by the individual institutions holding the data, both nationally and regionally.

Romania: In Romania, evidence from interview answers in this study suggest that administrative data are used for both monitoring and evaluation of ESF programmes, but there is no centralised system to access these data. Administrative data are stored by the individual institutions holding the data, and the procedure for gaining access differs depending on the processing purpose and the category of personal data. It was also reported that at national level, there is a lack of collaboration between institutions, and lack of coherent procedures and regulations concerning access to data.

Sweden: For Sweden, interviews for this study made it clear that access to administrative data for the purpose of monitoring and evaluating the ESF is centralised at SCB. SCB processes both data that are collected directly from participants by ESF beneficiaries, and data from administrative registers to link data of different datasets. The ESF managing authority, beneficiaries, and external evaluators can thereafter access administrative data from SCB for both monitoring and evaluation purposes. A document received from the Swedish ESF Council (the Swedish managing authority) explains in detail the past and current model for ESF and ESF+[376]. The document reports that the Swedish indicator model was introduced during the ESF programming period 2007-2013. The model implied that each ESF project reported participants' national personal identity numbers to SCB, which matched these against relevant administrative data. This system was developed under the ESF programming period 2014-2020 and will be further developed during 2021-2027. The managing authority has assessed this model as beneficial because it reduces the administrative burden for each project, increases protection of participants' personal data, secures the quality of reported indicators, and has a relatively low cost for monitoring and

[371] ANPAL (2023) Fse in Italia: https://www.anpal.gov.it/fondo-sociale-europeo

[372] Consultations, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 31 May 2023, and 06 June 2023

[373] European Commission. (2019b). *Pilot and feasibility study on the sustainability and effectiveness of results for European Social Fund participants using counterfactual impact evaluations: Final report*. p. 72.

[374] European Commission. (2021). *Design and commissioning of counterfactual impact evaluations : a practical guidance for ESF managing authorities*. https://data.europa.eu/doi/10.2767/02762, p. 38.

[375] European Commission. (2018b). *Study on the monitoring and evaluation systems of the ESF: Final report*. Annex 13: Country Report – Poland.

[376] *Svenska ESF-rådet, Svenska ESF-rådets indikatormodell för Europeiska socialfonden+ 2021–2027, Version 2, 2022 (Swedish ESF Council, Swedish ESF Council Indicator Model for the European Social Fund+ 2021-2027, Version 2, 2022)*.

evaluations. Moreover, with this model, each project reduces the amount of information that they need to collect from each participant (as SCB collects most information via administrative registers), reduces the risk for bias in data collection, and enables tracing of participants over time. For ESF+ 2021-2027, the SCB also has a new register on labour market status that will update data more frequently and increase efficiency because SCB will not need to collect data from other actors to the same extent as before. The ambition is to use as much administrative data as possible to reduce the number of surveys conducted.

Box 21: Key findings – Model of access to administrative data

- This study established that in most Member States the models for accessing and linking of administrative data for ESF/ESF+ monitoring and evaluation are not centralised nor harmonised.
- Sweden is the only example of a centralised and harmonised model of access to administrative data, where access to administrative data for ESF/ESF+ purposes is centralised at SCB.
- The other eight Member States (Austria, Germany, Spain, France, Ireland, Italy, Poland, and Romania) have decentralised models. In these Member States, there may be central databases containing data that are collected directly from the ESF/ESF+ participants and the managing authorities may play a coordinating role. However pre-existing administrative data that are used to complement and link data for monitoring and evaluation are neither coordinated nor processed centrally.

6.1.2. Access to administrative data in Austria

As explained above, Austria has **a decentralised model of access to administrative data for ESF/ESF+ monitoring and evaluation**. The Austrian managing authority (BMAW) has a coordinating role as it manages a central database containing data that are collected from the ESF/ESF+ participants. There is, however, no central institution that exclusively manages administrative data for ESF/ESF+ monitoring and evaluation.

According to a study published in 2019, the transfer of personal data to third parties was not allowed in Austria. Data could, however, be obtained in an anonymised form from the Safe Centres at Statistics Austria or remotely[377]. According to the same study, there was no information that unique identifiers were used to link administrative data. Instead, sector-specific identifiers were used, which are only used in certain branches and by certain authorities for official statistics[378]. In addition, according to an OECD study on impact evaluation of labour market policies using linked administrative data, central authorities, including Statistics Austria and the ministry responsible for labour, were responsible for linking unemployment registers with a number of other registers[379].

[377] European Commission. (2019a). *Pilot and feasibility study on the sustainability and effectiveness of results for European Social Fund participants using counterfactual impact evaluations : final report*. https://data.europa.eu/doi/10.2767/39339, p. 70.

[378] Ibid., p. 68.

[379]OECD. (2020). *Impact evaluation of labour market policies through the use of linked administrative data*. https://www.oecd.org/els/emp/Impact_evaluation_of_LMP.pdf , p. 48.

In the ESF context, a 2018 study found that in the programming period 2014-2020 **data** from existing administrative registers were **not used for monitoring purposes**[380]. The results of the interviews suggest that the same is still true for the new programming period 2021-2027. However, the managing authority is exploring the possibilities to access administrative data also for ESF+ monitoring purposes, especially for certain long-term result indicators[381].

In Austria, beneficiaries only collect data directly from participants[382]. No administrative data are collected by other organisations or government institutions for the purpose of ESF/ESF+ monitoring. All participant data (e.g., name, address, telephone number, e-mail, date of birth, social security number, nationality, mother tongue, highest level of education, current employment, employment status, education at project entry as well as special characteristics such as migrant/participant of foreign origin/members of minorities, participants with disabilities/other disadvantaged persons) are **collected via a central database** and in some cases via the separate project databases. The current database ZWIMOS[383], used in the programming period 2014-2020, has been modernised and further developed and this renewed database IDEA will be in place in the programming period 2021-2027. In the case of ethnicity as well as disability, the participants are allowed to leave this field open and use the option N/A (see also Section 5.4.3 above on the discussion of the fundamental freedom of confession in Austria).

This uniformed and central database is an electronic exchange platform for ESF/ESF+ purposes used by all beneficiaries and managed by the managing authority (BMAW)[384]. As explained by the interviewees, **the data** that feeds into this database **are collected directly from the participants through the ESF Master Data Sheet**[385]. Although this practice was closely examined with the idea of moving to the use of administrative data, it was decided that data should continue to be collected from participants via the Master Data Sheet. The reason for this is that many ESF/ESF+ indicators differ too much in definition from the administrative data in the national registers and some data are not available at all[386]. The managing authority considered that a combination of data collection from participants and administrative registers would be too time consuming[387]. Nevertheless, a change is proposed in the 2021-2027 programming period to collect a specific long-term result indicator from the social security register rather than from participants[388]. The reason for this change, which is currently under discussion, is to achieve a higher quality of data and not to impose an additional burden on participants.

While access to administrative data is restricted at the ESF+ monitoring stage, participants' data may be shared with project partners or subcontractors and with other governmental institutions or bodies. For such a transmission of data, the consent is sought from the

[380] European Commission. (2018b). *Study on the monitoring and evaluation systems of the ESF: Final report*. Annex 13: Country Report – Austria.

[381] Additional information provided by BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria).

[382] Interview, BFI Salzburg BildungsGmbH (ESF Beneficiary, Austria), 21 November 2022 and interview, ÖSB Consulting (ESF Beneficiary, Austria), 09 November 2022.

[383] See website: https://www.esf-projekte.at/prod/zwimos_userapp/.

[384] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[385] Interviews with BFI Salzburg BildungsGmbH (ESF Beneficiary, Austria), 21 November 2022, ÖSB Consulting (ESF Beneficiary, Austria), 09 November 2022 and BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[386] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[387] Idem.

[388] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022revealed that this change is still under consideration.

participants[389]. The data flow only happens in one-way as beneficiaries cannot obtain administrative data from these institutions[390].

The situation is different when administrative data are accessed **for ESF/ESF+ evaluation purposes**. Here, there are **several examples of the use of administrative data**. In the most recent ESF programming period 2014-2020, administrative data were used in two counterfactual impact evaluations (CIEs)[391]. The evaluators were able to access the necessary participants' data from the ZWIMOS database, but only in a pseudonymised form[392]. Consequently, in order for the evaluators to determine, for example, the employment history of the participants, the ESF/ESF+ data from the ZWIMOS database had to be linked and compared with data from the AMS-DWH database (Public Employment Service Data Warehouse). This was a rather complex process that also involved an external service provider in charge of **pseudonymisation**. A separate contract was concluded for such a purpose, which included provisions on the compliance with the data protection legal framework[393]. When the evaluation of the operational programme was done centrally by the ministry responsible for labour, the access to data was coordinated centrally within the ministry. By contrast, when the evaluations were done by the intermediary bodies, the access to administrative data was decentralised and managed solely by such bodies with some support from the ministry[394].

In summary, administrative data in Austria can mostly be accessed in a pseudonymised form and data can also be linked between different sources and databases. This is usually done by an external contractor, who is responsible for the linking of different datasets and the pseudonymisation process. In line with the data protection principle of minimisation, the amount and the type of data must be relevant and necessary to achieve the purposes. If aggregated data are sufficient, the processing of microdata is disproportionate[395]. This should be determined on a case-by-case basis.

One of the major challenges in Austria is to link data collected from participants with data on the participants from administrative registers. Identifying the person while respecting data protection rules is the key. While in other Member States the linking of data could be done on the basis of existing unique identifiers (e.g. social security codes, personal identification numbers) and then later pseudonymised using special identifiers, this does not seem to work in Austria. The Austrian DPA, for example, did not agree to the use of the national social security number as a unique identifier for ESF evaluation purposes in the 2014-2020 programming period, as this identifier is reserved for health measures[396]. A similar problem exists with the identifiers for labour market measures, which can only be used by the Public Employment Service[397]. According to Austrian data protection experts, **the use of sector-specific identifiers should be preferred** due to EU data protection rules. This means that **for ESF/ESF+ purposes, participants must be assigned a unique**

[389] Example of the master data sheet and accompanying data privacy notice for Salzburg state.

[390] A case of sharing data with the Chamber of Commerce's apprenticeship office was mentioned by one of the beneficiaries. Although the participants' data were sent to this office, the beneficiary was unable to obtain information from them on whether or not the participants had passed the qualification exams. Interview, BFI Salzburg BildungsGmbH (ESF Beneficiary, Austria), 21 November 2022 and interview, ÖSB Consulting (ESF Beneficiary, Austria), 09 November 2022. The Master Data Sheet used in Salzburg also indicates that certain participant data can be sent to the Public Employment Service.

[391] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[392] Idem.

[393] Intervention from the representative of the Austrian managing authority during the Focus Group, 16 March 2023.

[394] Additional information provided by BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria).

[395] Additional information provided by BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria).

[396] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[397] Intervention from the representative of the Austrian managing authority during the Focus Group, 16 March 2023.

identifier so that their data can be located in the registers. As there is currently no such identifier for ESF/ESF+ purposes, participants have to be identified through a multi-level process using several pieces of personal data (e.g. name, date of birth)[398]. The managing authority is currently working on the creation of a new unique identifier that could be used during the ESF+ programming period[399], but this is not a straightforward process as sector-specific identifiers are not used in other existing administrative databases[400].

Once the solution to the identifiers for linking data has been found, the managing authority expects to use further administrative data in the current programming period, in particular data from the Public Employment Service Data Warehouse (AMS-DWH), employment status and income data from the Main Association of Social Insurances and perhaps even certain school statistics (BilDok, BibEr)[401].

Box 22: Key findings – Access to administrative data in Austria

- Austria has **a decentralised model** of access to administrative data for ESF/ESF+ monitoring and evaluation. The Austrian managing authority (BMAW) has a coordinating role as it manages a central database containing data that are collected from the ESF/ESF+ participants.
- **Access to administrative data for monitoring purposes is very limited**. Data are collected directly from the participants through the ESF Master Data Sheet and stored in an electronic database called ZWIMOS (in 2014-2020) and IDEA (in 2021-2027). In 2014-2020, very little data was collected from administrative registers as the managing authority found that the definitions of too many ESF/ESF+ indicators differed from the definitions of administrative data in the national registers and some data were not available at all. This may change in the 2021-2027 programming period, as the managing authority is considering collecting a specific long-term result indicator from the social security register rather than from participants in order to achieve a higher quality of data and not to impose an additional burden on participants.
- Access to administrative data is more common for evaluations. Experience shows that administrative data can mostly be accessed in a pseudonymised form and can be linked between different sources and databases, usually with the help of an external contractor. Although access to data is possible, the main issue is that Austrian data protection experts insist that sector-specific identifiers should be used instead of common unique identifiers. As there are currently no unique identifiers for the ESF+ purposes, data linkage is a resource-intensive process.

6.1.3. Access to administrative data in Spain

According to a study published in 2019, the Spanish Data Protection Law limits access to administrative data, and one of its implications is that the Public Employment Service can

[398] *Austrian Institute for Economic Research, Das Operationelle Programm "Beschäftigung Österreich 2014 bis 2020" des Europäischen Sozialfonds, Endbericht der begleitenden Evaluierung, March 2022, pp. 156-157.*

[399] Idem.

[400] Additional information provided by BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria).

[401] Idem.

only access information from the Social Security Administration on employment status individual by individual[402],which is time consuming. Unique identifiers are used (ID card numbers), but these are not always linked to other administrative data[403]. According to the UAFSE, limitation to the access to administrative data is always linked to the typology of the data. In order to manage sensible data, it is compulsory to comply with the national rules on Data Protection[404].

There are previous successful examples of the use of administrative data for an ESF counterfactual impact evaluations in Spain[405], and the interviews conducted as part of this study identified several examples of the use of administrative data, both for ESF/ESF+ monitoring and evaluation.

Based on the interviews with Spanish stakeholders the data flow, including the access to administrative data, for the purposes of ESF/ESF+ monitoring and evaluation can be described as follows.

According to UAFSE[406], a specific feature identified in Spain is the **decentralisation of the collection of data** for the monitoring and evaluation of the different programmes by the various Autonomous Communities and Regional Authorities, as they all act as intermediate bodies. UAFSE normally externalises ESF monitoring and evaluation activites. Consequently, UAFSE uses the aggregated data provided by the different intermediate bodies. These data can be defined as figures on the employment or education situation of the participants, as well as data disaggregated by gender. ESF+ Managing Authorities and evaluators, whether external or not, use the databases of the Public Employment Services and the Ministry of Education to report and inform on the employment and education situation of programme participants. In fact, the monitoring of the implementation of the programmes is reported annually in the Annual Implementation Report (one per programme), for which the aggregated data are provided by the intermediate bodies. Systematic, operational or thematic evaluations are normally carried out externally under the supervision of the UAFSE. The method of data collection is indicated in each evaluation, although the starting point is usually interviews and surveys with each intermediate body and/or the beneficiaries, the actual implementers of the actions.

According to UAFSE, special agreements are in place between national stakeholders for access to admistrative data for ESF monitoring and evaluation. Spanish Managing Authorities used to take into account recommendations from the Institute for Fiscal Studies (Instituto de Estudios Fiscales[407]) depending on the Ministry of Internal Revenue Services and Public Administrations. It is one of the main stakeholders regarding evaluation and studies for public administrations. Normally this public institution elaborates Ex ante evaluations of Operational Programmes and Counterfactual evaluations and offers training and support on evaluation methodologies and definition of indicators, among others.

UAFSE also confirmed in the interview that special categories of personal data require the consent of the individuals concerned in order to be used. This means that UAFSE analyses administrative data for the purpose of monitoring and evaluation of the programmes, but with regard to special categories of data (ethnic or religious origin, disability, sexual orientation, genetic or biometric data, health conditions, data concerning children, etc.),

[402] European Commission. (2019b). *Pilot and feasibility study on the sustainability and effectiveness of results for European Social Fund participants using counterfactual impact evaluations: Final report*. p. 71.

[403] Ibid., p.68.

[404] Interview, Spanish Administrative Unit of the European Social Fund (UAFSE), 26 June 2023.

[405] European Commission. (2021). *Design and commissioning of counterfactual impact evaluations : a practical guidance for ESF managing authorities*. https://data.europa.eu/doi/10.2767/02762, pp. 92-93.

[406] *Spanish Administrative Unit of the European Social Fund (UAFSE)* https://www.mites.gob.es/uafse_2000-2006/uk/bienveni.htm.

[407] IEF – Instituto de Estudios Fiscales: https://www.ief.es/

special attention should be paid to compliance with data protection rules. In this respect, the UAFSE points out that there are limitations depending on the nature of the data. According to the legal provisions, all final ESF recipients consented for their data to be used for the purposes of ESF information and evaluation and at evaulation level their sensitive data do not appear individually. Therefore, the UAFSE considers that in practice, based on its previous experience in programme management, the tools to obtain data for the purpose of monitoring or evaluations are usually surveys, interviews, and consultations during open processes in which the parties involved in the management of the ESF/ESF+ can intervene.

If some specific data are needed to carry out an administrative act, they are **collected directly from the interested party**. Otherwise, the interested party provides this information directly. In order to have access to administrative data for the monitoring or evaluation processes in the context of ESF+ programmes, this interested party **must comply with various legal criteria and with the security measures** foreseen in the Security Document (Annex II and following) and in the Spanish Royal Decree 3/2010, of 8 January, which regulates the “National Security Scheme”.

Another beneficiary, the *Mancomunidad Intermunicipal Alto Palancia,* stated that certain data need to be requested from interested parties, which takes about 10 days. Therefore, it does not achieve maximum efficiency in the management of such data. Access to the vast majority of administrative data (economic, social, family, etc.) requires the consent of the data subject. In order to meet this challenge, they propose to ask the data subjects for their consent in advance. This would allow files to be processed in a timely manner.

An interview with an evaluator Red2Red confirmed that the data used to evaluate ESF/ESF+ come from the competent bodies managing the programmes and from regional or national public administrations. Ad hoc agreements on access to administrative data are established for each evaluation. The evaluators can obtain both socio-economic data (e.g., age, level of education, employability, gender), as well as monitoring data (number of people participating in a given measure). Examples of administrative data obtained from public registers include public registry data (births, marriages and deaths), immigration records, employment/jobseeker records (including PES and participation in vocational training), school or education records, social service records, etc. According to Red2Red, there are no restrictions on the access or use of administrative data for ESF+ purposes as these **data are aggregated or anonymised**.

The difficulty stems from the fact that **evaluators can only access the data provided for in the ESF+ Regulation**, without the possibility of analysing other types of data beyond what is necessary to carry out their activity (sensitive indicators related to homeless people or people with difficulties)[408]. Further access would also contravene national data protection legsilation[409]. In the opinion of Red2Red, this type of information would have been relevant to carry out more holistic analyses. For example, in the case of public registry data (births, marriages, and deaths), only country of origin is included; in the case of health records, only whether or not the persons has a disability is included; in the case of school or education records/registers, only the level of education is included. It should be highly relevant to include data related to tax registers, especially income level.

Another challenge is also **the length of the anonymisation process**. It takes a long time for data to be anonymised and transferred. There is a **need for greater uniformity and coherence** of the above-mentioned pioneering regional with the central administration and the remaining regions.

[408] Interview, Red2Red (Spanish Consulting company), 19 October 2022.

[409] Consultation, UAFSE - Spanish Administrative Unit of the European Social Fund (managing authority, Spain), 25 May 2023

The Spanish Data Protection Authority (AEPD) has an extensive list of guides, reports, and documents on the processing of personal data by public administrations[410].

In summary, there is no centrally managed system for access to administrative data in Spain and administrative data are stored by the individual institutions that hold the data. There is a decentralised management under common and uniform parameters[411]. It should be noted that data holders are in many cases the regions themselves.

Box 23: Key findings – Access to administrative data in Spain

- In Spain, there is no centrally managed system for accessing administrative data but rather a decentralised management governed by common and uniform parameters Data holders are in many cases the regions themselves.
- The collection of data for the monitoring and evaluation of the different programmes is decentralised among the different Autonomous Communities and Regional Authorities, as they all act as intermediate bodies. Consequently, the managing authority uses the aggregated data provided by the different intermediary bodies.
- Special categories of personal data may not be processed, even in anonymised form, due to data protection restrictions. The consent of the individual is required to process such data.
- From the interviews conducted for this study, there is a clear need for greater uniformity and coherence of the regional models, as well as a more efficient interaction with the central administration.

6.1.4. Access to administrative data in Italy

Although it is not possible to identify a single model for the purposes of ESF/ESF+ monitoring and evaluation, there is considerable experience in Italy of accessing administrative data for monitoring purposes and conducting evaluations by using administrative datasets. The Italian DPA has not provided any general guidance relevant to the use of personal data collected for the purposes of monitoring and/or evaluation of ESF/ESF+ programmes.

For ESF/ESF+ monitoring and evaluation, each managing authority (national and regional) is responsible for collecting and storing microdata on participants in ESF/ESF+ measures. In some cases, **administrative datasets (from regional employment and training records) are used to complement participants' data**.

[410] (1) *Agencia Española de Protección de Datos (AEPD), Publicaciones y resoluciones*. https://www.aepd.es/en/publicaciones-y-resoluciones (2) *Agencia Española de Protección de Datos (AEPD), Administraciones Públicas*. https://www.aepd.es/es/areas-de-actuacion/administraciones-publicas

[411] According to the Spanish Administrative Unit of the European Social Fund (UAFSE), common orientations are described in the documents of management and control systems that each Operational Programme has and on their Evaluation Strategies. The ESF Spanish Deputy Director for Programming and Evaluation is the Unit dealing with evaluation systems and strategies for each ESF Programme. Concerning the Monitoring activity, each Programme has constituted a Monitoring Committee in charge of analysing the progresses and accomplishment of the milestones and goals stablished.

There is also a **central harmonised dataset for the implementation of cohesion policy** (*Banca Dati Unitaria* – BDU[412]) managed by the General Inspectorate for Financial Relations with the European Union (IGRUE) of the Ministry of Economy and Finance[413] (MEF) within the **National Monitoring System**. To this database, the managing authorities are required to submit information on the physical, financial, and procedural progress of the financed projects every two months through their local information systems. However, this information does not necessarily contain personal data[414].

The lack of a harmonised dataset at national level at the level of participants, makes it difficult to link and use data for ESF/ESF+ monitoring and evaluation at the national level.

ANPAL[415], a national managing authority, uses administrative data for both monitoring and evaluation of ESF/ESF+ programmes under its remit. Indeed, ANPAL's Information Systems Division 7[416] manages the SIU and allows ANPAL's research structures (authorised staff) access to anonymised data for monitoring and evaluation purposes. No particular restrictions have been identified in accessing or using administrative data for monitoring and evaluating the ESF. The access to administrative data is done principally in an inner database, which has no restrictions to internal authorised employees. During the management and control phases the queries to administrative database of other Public Administrations are done based on special agreements[417], which safeguard all the European and national rules concerning personal data protection. In the management phase, ANPAL has access to several administrative registers, such as the employment/jobseeker registers for employment data on participants[418].

ANPAL is the managing authorithy of the National Operational Program Youth Employment Initiative (YEI) and the 21 Italian Regions are Intermediary bodies. As of 2014 (the starting point of the Youth Guarantee in Italy), ANPAL has coordinated and centralised **for the first time** a national administrative dataset Sistema informativo unitaro (SIU) which collects regional administrative data on participants and labour market policies. A standard data record (*SAP-Scheda anagrafico professionale sezione 6*) has been shared and implemented with the regions. According to legislative decree 150/2015, SIU also collects administrative data on mandatory communication on employment (*Comunicazioni obbligatorie*) and Declaration of Immediate Availability to work *(Dichiarazione di immediata disponibilità*) of people who participate in a labour market policy or go to a public employment service to get a new or different job. This administrative data set has allowed

[412] At the heart of the National Monitoring System is the Unified Data Bank (UDB), fed at the individual project level by the Local Information Systems of all the Administrations in charge of Plans or Programmes financed by cohesion resources on the basis of shared rules and standards. See (1) *Coesione Italia, Sistema Nazionale di Monitoraggio*. https://opencoesione.gov.it/it/sistema_monitoraggio/ (2) *Ministero dell'Economia e delle Finanze, La trasmissione dei dati*. https://www.rgs.mef.gov.it/VERSIONE-I/attivita_istituzionali/monitoraggio/spesa_per_le_opere_pubbliche/la_trasmissione_dei_dati/

[413] *Ministero dell'Economia e delle Finanze, home page*. https://www.mef.gov.it/

[414] Interview, Ministry of Economy and Finance – IGRUE (Administrative Data Holder, Italy), 26 October 2022.

[415] ANPAL is the National Agency for active labour policies. It promotes people's right to work, training and professional growth, coordinates the national network of employment services and is responsible for the labour market information system. Available at: https://www.anpal.gov.it/chi-siamo.

[416] From an organisational point of view ANPAL is divided into (i) 4 Research Structures and (ii) 7 Divisions (Divisioni). Both components report to a Director General. The Research Structures are staffed by researchers, technologists and research collaborators whose activities are defined each year in specific Research Activity Plans separate from the Agency's general Integrated Operational Plan. For this reason, the monitoring and evaluation activities of the Research Structures are assimilated to the scientific production of the research organisations. The Research Structures carry out monitoring and evaluation of employment policies, financed or not by the ESF, on the basis of Legislative Decree 150/2015 (Article 16) and therefore have access to ANPAL's administrative data (SIU).

[417] As an example, in the case of PON IOG (National Operational Programme Youth Employment Initiative), ANPAL has an agreement with the MIUR for the sole purpose of verifying the NEET status of young people registered in the Programme (massive verification of data by means of a Fiscal Code, whose only feedback from the MIUR is a 'Yes/No' response) for reporting purposes. While for evaluation purposes the request to MIUR for detailed data on the return to the education system of the young person who has completed the Youth Guarantee policy has not yet been finalised.

[418] Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF Managing Authority, Italy), 03 November 2022.

the monitoring and evaluation of the YEI Program to be carried out, in particular effectiveness evaluation with counterfactual impact approach. For evaluation purposes of the YEI Program, the ALMP Evaluation Unit of ANPAL (*Struttura1*) has access to this dataset. In order to report on financial expenditure made by the regions as intermediary bodies of the YEI Program (according to the EU regulation), ANPAL has signed an agreement with the Ministry of education to make a check on the actual NEET status of young people registered in the programme[419].

The Marche Region[420], a regional ESF/ESF+ managing authority, can also **access several administrative datasets for both monitoring and evaluation purposes**[421]. For example, an administrative dataset of the regional JOB Agency is used to calculate the gross employment rate of participants and to thus calculate the ESF/ESF+ operational programme results indicators on participants in employment, including self-employment, six months after leaving the programme. The monitoring data collected from ESF/ESF+ participants are linked to the JOB Agency dataset through a unique identifier (the Italian fiscal code) in the form of a tax/social security number for the assessment of the duration of unemployment and for impact analyses using counterfactual methods[422]. **Data may be provided to external evaluators in anonymised form**, but this is not always the case. If the data are not anonymised, they are subject to data protection protocols and may only include subsamples of variables[423]. For evaluation purposes, the Marche Region also uses data from the COMarche dataset, which includes information on the employment history of individuals by gender, age, education, citizenship. The ASIA dataset (the companies' statistical register), managed by the Italian statistical institute, is also used, which contains information on the sector of activity and number of employees[424].

A concrete example of how data is stored in Italy comes from the interview with the ESF+ beneficiary IAL FVG[425], which has its own internal digital management system (Ial Man) that records and makes available all the data needed for the implementation of ESF/ESF+ projects. IAL FVG relies on a data centre located in Milan, which takes care of all back-ups and security solutions. IAL FVG, which collects information directly from ESF/ESF+ project participants, **can also access personal data from other organisations through an interoperability system** that allows the employment centres (*Centri per l'impiego*) to digitally transfer the user's data to the operators in charge of professional education in the region.

In Italy, access to non-anonymised data is not possible for "external" users (including evaluators). However, **administrative data are** still **used to carry out evaluations**. In some cases, regional offices have the capacity to integrate the databases needed to carry out a CIE[426]. Although administrative data, such as on employment, are managed at a regional level, there are examples, such as from the Province of Trento, where evaluators have been able to merge these data with national tax return registers[427].

[419] Consultation, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 31 May 2023

[420] *Regione Marche, Home Page*. https://www.regione.marche.it/

[421] Interview, Marche Region (ESF managing authority, Italy), 21 October 2022.

[422] Interview, Marche Region (ESF managing authority, Italy), 21 October 2022.

[423] Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 03 November 2022.

[424] *Istat - Istituto Nazionale di Statistica, Scheda standard di qualità - registro statistico delle imprese attive (ASIA - IMPRESE)*. Retrieved 2023 from https://www.istat.it/it/archivio/216767

[425] *IAL FVG, IALweb*. https://www.ialweb.it/

[426] European Commission. (2019b). *Pilot and feasibility study on the sustainability and effectiveness of results for European Social Fund participants using counterfactual impact evaluations: Final report*.

[427] European Commission. (2021). *Design and commissioning of counterfactual impact evaluations : a practical guidance for ESF managing authorities*. https://data.europa.eu/doi/10.2767/02762, p. 38.

Two different models at regional level for using administrative data for the purposes of ESF/ESF+ monitoring and evaluation were identified in the Veneto and Umbria regions.

Box 24: Example from the Veneto region

'Veneto Lavoro'[428] was established under Article 8 of Regional Law No 31/1998 and is governed by Articles 13 to 19 of Regional Law No 3/2009 'Provisions on employment and the labour market'. It is an instrumental body of the region, with legal personality under public law and with organisational, administrative, accounting and patrimonial autonomy. In particular, Veneto Lavoro, is a regional body to which the functions of management, operational coordination and monitoring of the public employment services network and human resources' management of the public employment service network have been assigned in accordance with Article 13(2) of the Regional Law No. 3/2009. All the services provided by Veneto Lavoro are available at: www.cliclavoroveneto.it

Veneto Lavoro makes available to researchers and research bodies, on the basis and for the sole purpose of carrying out a research project, the basic data collected by the Veneto Employment Centres through the public use file called '**Mercurio'**[429].

Mercurio is the statistical database (the third version) that the Veneto Lavoro Observatory places at the disposal of researchers in the form of a **public use file (Puf)** in order to allow them to make full use of the wealth of information that comes from the administrative management system of the Employment Centres, a system that organises the flows of compulsory communications and declarations of availability for work made by workers.

The turning point that brought about a radical change in the organisation of the information received by the Employment Centres on labour relations was the introduction of the **Compulsory Communications system**[430] (Sistema delle comunicazioni obbligatorie) at national level and, for the Veneto region, the adoption of the **Veneto Lavoro Information System (Silv)** [431].

The following organisations can request data from the Mercurio database: universities, research institutes or bodies (public or private), scientific societies and researchers working in their field. The procedure to be followed and requirements are explained here: https://www.venetolavoro.it/public-use-file.

Veneto Lavoro published a 'Guideline to Mercurio'[432] in December 2021.

[428] *Veneto Lavoro, Veneto Lavoro*. https://www.venetolavoro.it/chi-siamo

[429] *Veneto Lavoro, Come richiedere Mercurio*. https://www.venetolavoro.it/contenuti-del-sito/-/asset_publisher/kB7hwylekZ1z/content/come-richiedere-mercurio

[430] *Ministero del Lavoro e delle politiche sociali, Computer System for Compulsory Communications, Sistema informatico per le comunicazioni obbligatorie*. https://www.co.lavoro.gov.it/co/welcome.aspx

[431] *Veneto Lavoro, Sistema Informativo Lavoro Veneto*. https://www.venetolavoro.it/silv

[432] *Osservatorio Mercato del Lavoro: PUF 4.0 – GUIDA A MERCURIO Storia, contenuto e specifiche*. (2021). Veneto Lavoro Retrieved from https://www.venetolavoro.it/documents/10180/16486105/PUF+Mercurio+-+guida+all%27uso+%28ver+2021-12%29.pdf/b0b25409-6d79-2579-b105-a62e93767a32?t=1640170964620

Box 25: Example from Umbria

The managing authority of the ESF Operational Programme 2014-2020, in order to ensure that all the exchanges of information with the beneficiaries are carried out through electronic data exchange systems, has equipped itself with a specific regional IT system to support the 2014-2020 programming period, called SIRUFSE 14-20.

SIRU-FSE enables the management and monitoring of the programming processes of the 2014-2020 ESF operational programmes, in accordance with the provisions of the IGRUE National Monitoring System (SNM)[433] and in compliance with the Single Conversation Protocol (PUC).

The system allows for the computerised collection, recording and storage of data on individual operations for the purposes of their monitoring, evaluation, financial management and verification.

The public part of the SIRUFSE 14-20, called 'Siriwebfse1420'434, which is the main mechanism for collecting the data needed to manage and monitor activities, is accessible via https://siruwebfse1420.regione.umbria.it/.

It can be accessed using the SPID (Sistema Pubblico di Identità Digitale) digital identity.

The system can be accessed by the staff of any organisation (training organisation, company, public body, etc.) authorised to enter, modify, consult and officially transmit data on the projects they manage.

To conclude, the managing authorities ANPAL and Marche Region did not mention any major challenges related to access to administrative data. However, **it is not always possible to access the full set of data** requested[435]. In addition, ANPAL described that it can be a challenge to comply with both EU and national data protection legislation, in particular data processing related to Articles 9 (processing of special categories of data) and 10 (processing of personal data relating to criminal convictions and offences) of the GDPR. Another challenge is the interconnection between different information systems[436]. Beneficiary IAL FVG mentioned that they do not face any challenges related to data protection. However, one challenge concerns the lack of interoperability between regions and the national level.

Box 26: Key findings – Access to administrative data in Italy

- From the interviews conducted for this study, it can be confirmed that regional Managing Authorities, such as the Marche Region, have on several occasions used administrative data from regional datasets for ESF monitoring and evaluation, while the national managing authority has special agreements, in

[433] *General Inspectorate for Financial Relations with the European Union (IGRUE), IGRUE-Ispettorato Generale per i Rapporti finanziari con l'Unione Europea*. https://www.rgs.mef.gov.it/VERSIONE-I/e_government/amministrazioni_pubbliche/igrue/index.html

[434] *Regione Umbria, SiruWEB*. https://www.regione.umbria.it/por-fse/siru-fse

[435] Interview, Marche Region (ESF managing authority, Italy), 21 October 2022

[436] Interview, Innovazione Apprendimento Lavoro Friuli Venezia Giulia (ESF Beneficiary, Italy), 26 October 2022

accordance with data protection rules, to access the administrative data needed from other public bodies.

- Administrative data are also used for evaluations also by external evaluators, either in the form of anonymised or non anonymised data. Ease of access to non anonymised data -- subject to data protection protocols - might differ according to the data owner. Where data are not anonymised, they mostly include subsamples of variables.

- Access to participants' and administrative data differ between the national and regional levels, and requirements might change with each region/data holder. Although there is an example of a central harmonised dataset at the national level for the implementation of cohesion policy, such data do not necessarily include personal data, and it may be difficult to link and use data for ESF/ESF+ monitoring and evaluation at a national level.

6.2. Legal obligations and conditions to access data

This section begins by outlining the legal obligations arising from EU law when accessing individual-level administrative data for ESF/ESF+ evaluation and monitoring purposes (Section 6.2.1) and continues by analysing the legal obligations and conditions to access administrative data in three Member States, namely Austria, Spain, and Italy (0 to 6.2.4). The analysis focuses on any differences in access to administrative data depending on: (i) the use of data (evaluation vs. monitoring); (ii) the sector of the user (evaluator) requesting access to data (e.g. academia, governmental bodies, private bodies or non-governmental organisations); (iii) the age of the data subject (children vs. adults); (iv) the residency of the evaluators (local vs. foreign evaluators); or the hosting of data (data hosted by the statistical office or another body).

6.2.1. Legal obligations arising from the EU law and their national implementation

As explained in Section 5.1.2, Article 4 of the CPR 2021 and Article 17(6) of the ESF+ Regulation are the main provisions governing access to administrative data for the ESF+ monitoring and evaluation. While Article 4 of the CPR 2021 is a general provision allowing Member States to process personal data for ESF+ monitoring and evaluation purposes, Article 17(6) of the ESF+ Regulation is more specific and allows Member States to enable competent authorities to access data from national administrative registers on the basis of national provisions establishing a legal obligation or a task carried out in the public interest, which necessitates such processing of personal data.

In addition, Article 44 of the CPR 2021 provides for rules on the evaluations by the Member States. Paragraph 1 obliges the Member States or their managing authorities to carry out evaluations of the programmes with a view to improving the quality of the design and implementation of programmes. In order to be able to do so, paragraph 4 requires Member States or managing authorities to ensure that the necessary procedures are put in place to produce and collect the data required for evaluations. Article 69(4) of the CPR 2021 also requires the Member States to ensure the accuracy and reliability of the monitoring system and of data on indicators.

In order to understand how access to existing administrative data for ESF/ESF+ monitoring and evaluation purposes takes place in a national context, knowledge of national administrative and data protection legislation and practices is needed.

The main difference in the **use of administrative data for evaluation and monitoring purposes** is that evaluations may require access to existing data of third parties not involved in ESF/ESF+ programmes. As already discussed in Section **Error! Reference source not found.** the processing of non-participants' data, in particular in the case of counterfactual evaluations, raises questions regarding the reuse of data in situations (i) where data originally collected for purposes other than participation in ESF+ projects are reused on the basis of a new legal basis; and (ii) where data collected are used for additional/further purposes, but based on the same legal basis.

The sector from which the evaluator originates, may also have an impact on the access to data. For example, national data protection legislation may distinguish between processing carried out by or on behalf of public and private bodies[437] or even between individual bodies. An example of the latter is the LIL in France, which only allows processing for statistical purposes if it is carried out by the Institute for National Statistics and Studies or by a ministerial statistics body (Article 44(2) LIL), while Article 44(6) of the LIL may allow reuse of data for scientific research by certain public bodies. As mentioned in Section 5.2.2, national rules on the processing of data for scientific research purposes may be less strict for certain evaluators.

The **age of the data subject** could also be an important factor, as the GDPR explains that children merit special protection with regard to their personal data[438]. Typically, this means that the consent of the holder of parental responsibility is required when processing children's data, and that all information and communications regarding the processing of children's data must be in clear and plain language. The GDPR, however, provides for specific rules on the lawfulness of processing based on consent only in relation to information society services offered directly to a child (Article 8 GDPR). National administrative, civil or data protection law may provide for additional safeguards for the processing of children's data (e.g. authorisation of the holder of the parental responsibility, possible age limit, transparency obligation).

The residence or location of the evaluators may also play a role. Although the GDPR promotes the free flow of personal data within the EU/EEA legal area[439], any transfer of data to an evaluator established in a third country[440] is only possible if the level of protection guaranteed by the GDPR is not undermined by such data transfer, including in cases of onward transfer[441]. To this end, the GDPR provides for a three-step approach to determine the legal instrument that would facilitate the transfer of data to third countries or international organisations. In the absence of an adequacy decision (Article 45 GDPR) or of appropriate safeguards such as standard contractual clauses, binding corporate rules, codes of conduct and others (Articles 46-48 GDPR), data may still be transferred by virtue of a derogation (Article 49 GDPR). In addition, Member States have a margin of manoeuvre to restrict the free flow of personal data. Such restrictions could be physical localisation requirements on the national territory, legal requirements (e.g., the need to ensure national supervision) or technical requirements (e.g., storage within a specific secure zone or disaster recovery requirements).

[437] Examples include the German BDSG that distinguishes between processing for public authorities and for private entities and Section 2 of the Dutch GDPR implementation act.

[438] GDPR, recital 38.

[439] GDPR, Article 1(3).

[440] As the GDPR has been incorporated into the EEA Agreement, third countries are considered those countries outside the EEA.

[441] GDPR, recital 101.

Finally, the difference in access to administrative data may arise from the **type of body hosting the data** (e.g. data hosted by the national statistical office and/or another government body). Even if the legislation on the access to data is universal, such a difference may arise for practical reasons, such as the existence of data sharing agreements. Only the parties to such an agreement can transmit administrative data between themselves. In addition, when access to data is requested from a body within the same ministry, access appears to be less cumbersome in practice.

Box 27: Key findings – Legal obligations and conditions for access to data

- Article 4 of the CPR 2021 and Article 17(6) of the ESF+ Regulation are the main provisions in EU law governing access to administrative data for the ESF+ monitoring and evaluation. Both provisions remain very general, leaving it to the Member States to provide for more specific rules for the reuse of administrative data in line with the GDPR.
- National data protection legislation may also affect the way in which data can be accessed. National data protection legislation may distinguish between processing carried out by or on behalf of public and private bodies, or even between individual bodies, between the processing of participant and non-participant data, by the age of the data subject, and by the location of the evaluators.
- Finally, national practice may also play a role, as the conclusion of data sharing agreements or the relationship between certain national actors may also facilitate easier access to administrative data.

6.2.2. Legal obligations and conditions to access data in Austria

The legal research did not find any national rules or obligations that would create different conditions for access to data for ESF/ESF+ monitoring and evaluation purposes. This was confirmed by an interview with the Austrian DPA, which indicated that no guidelines or decisions had been adopted regarding the use of personal data for the purpose of monitoring and evaluation of the ESF/ESF+ programmes or regarding the reuse of administrative data in this context. As explained by the managing authority, administrative data have not been used for monitoring purposes in the 2014-2020 programming period. However, the reasons for this are not related to national legal obligations and conditions, but to practical considerations (e.g. different definitions of indicators, time-consuming process).

A general legal basis for the exchange of data between public authorities in Austria is provided by Section 17 of the E-Government Act (*E-GovG*)[442], which enables public authorities to use data from existing electronic registers in the public sector. However, this legal basis is not used for access to administrative data for ESF+ monitoring and evaluation

[442] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG) StF: BGBl. I Nr. 10/2004 (NR: GP XXII RV 252 AB 382 S. 46. BR: 6959 AB 6961 S. 705.), RIS - E-Government-Gesetz - Bundesrecht konsolidiert, Fassung vom 11.04.2023 (bka.gv.at). Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG) StF: BGBl. I Nr. 10/2004 (NR: GP XXII RV 252 AB 382 S. 46. BR: 6959 AB 6961 S. 705.), RIS - E-Government-Gesetz - Bundesrecht konsolidiert, Fassung vom 11.04.2023 (bka.gv.at).

purposes[443]. In general, the reuse of administrative data for ESF/ESF+ monitoring and evaluation in Austria is legitimised by the following legal provisions: (i) Article 44(1) CPR 2021 (previously Article 54(1) CPR 2013); (ii) legal bases for processing of personal data in Article 6(1)(c) and (e) of the GDPR; and (iii) explicit consent if it is necessary to link special categories of personal data[444]. There is no general provision in the Austrian Data Protection Law (*Datenschutzgesetz* – DSG) allowing access to administrative data at the individual level. Furthermore, there are no other national acts or instruments, such as agreements between public authorities which are relevant for access to existing administrative data.

Although the Austrian administration has a good base of central registers and (internal) databases, including partly structured and unstructured data, the underlying potential for optimisation does not seem to be fully exploited[445]. For natural persons, the main register is the Central Civil Status Register, which is linked to the Central Register of Residents, while for legal persons it is the Company Register, which is linked to the supplementary register of other interested parties. Although the technical interfaces for the exchange and transmission of administrative data are in place, they do not seem to be suitable for regular communication between the authorities[446]. The main problem is the existence of more than 100 registers with different data quality and each with a large number of technical interfaces[447]. The Register- und Systemverbund (RSV), developed by the Austrian Federal Computing Center, aims to improve the exchange of data between national public bodies[448].

While there are no differences in terms of the sector of the user (evaluator) requesting access to data (e.g. academic organisation, government body, private entity, non-governmental organisation), there are **some differences in the legal obligations and conditions for access to data with respect to the purpose of data use**.

For example, the use of data for research could fall under the provisions of the Research Organisation Act (*Forschungsorganisationsgesetz*)[449]. This Act regulates access to administrative data in the context of a research project in accordance with Article 89 of the GDPR on the processing of data for archiving, scientific or historical research and statistical purposes. Section 2b.(1) regulates which persons and organisations may receive and use "specific personal identifiers". In addition to museums and universities, these could include, among others:

- natural persons, associations of persons as well as legal entities that receive Article 89 funds from the Austrian Science Fund (Article 2 of the Research and Technology Promotion Act (Forschungs- und Technologieförderungsgesetz - FTFG)) or within the framework of the European Framework Programmes for Research and Development; and

[443] Additional information provided by BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria).

[444] Additional information provided by BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria).

[445] *Federal Ministry of Digitisation and Economic Location (Bundesministerium Digitalisierung und Wirtschaftsstandort), Konzept: Register- und Systemverbund (RSV) als Attributs-provider bzw. -Handler insbesondere zur Umsetzung des Once Only-Prinzips in der österreichischen Verwaltung, 18 October 2018*. P.2

[446] Ibid.

[447] Ibid., pp. 3, 5 and 6.

[448] Idem.

[449] Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation (Forschungsorganisationsgesetz – FOG) StF: BGBl. Nr. 341/1981 idF BGBl. Nr. 448/1981 (DFB) (NR: GP XV RV 214 AB 778 S. 81. BR: S. 413.) (Federal law on general matters according to Art. 89 GDPR and the research organization (Research Organization Act – FOG)). https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009514.

- 'public bodies' which are entrusted by law with tasks pursuant to Article 89 of the GDPR.

'Public bodies' are defined in Section 4 of the Information Use Act (*Informationsweiterverwendungsgesetz*). They include the federal government and other public bodies under Austrian law. They do not include foreign entities. Interventions by the Austrian managing authority during the focus group meeting suggested that this legal basis could not be used for the purpose of **ESF/ESF+ evaluations, as they do not qualify as scientific research** under the conditions of this Act. The Research Organisation Act therefore does not provide for a legal basis for access to administrative data by the ESF/ESF+ evaluators.

The review of legal documents relevant for access to administrative data did not reveal any difference in access based on the age of the data subject (children vs. adults). However, it seems that in practice **personal data of pupils could not be used for evaluations**. To overcome this problem, data on whole classes were used instead[450].

Similarly, the review of national rules did not reveal any significant differences regarding access to data based on the residence of the evaluators (local evaluators vs. foreign evaluators). However, it should be noted that specific legislation may give fewer rights to foreign entities. For example, the Research Organisation Act (*Forschungsorganisationsgesetz*) clarifies that public authorities within the meaning of the Act are only national and not foreign authorities. As explained above, this Act does not provide a valid legal basis for access to administrative data for ESF+ purposes.

In principle, **all types of actors could have access to administrative data** for ESF/ESF+ monitoring or evaluation purposes (e.g. managing authorities, external evaluators, intermediary bodies). Access to data does not depend on the type of actor accessing the data but rather on the legal basis for the use of administrative data. For example, a managing authority may access administrative data for monitoring purposes on the basis of the provisions of the ESF+ Regulation, while the intermediary body is obliged to access administrative data due to the evaluation obligation.

On the other hand, there **may be differences depending on the body hosting the data** (data hosted by the statistical office or another body). Although, from a legal point of view, the general rules on access to administrative data are uniform for all bodies, specific rules on access might apply in the case of certain bodies. For example, in the case of access to statistical data of Statistics Austria (*Statistik Austria*)[451], the Federal Statistics Act (*Bundesgesetz über die Bundesstatistik*)[452] provides for specific rules for the use of statistical data for scientific research purposes. If ESF/ESF+ evaluators wish to have access to statistical data for research purposes, they would have to prove that their evaluations meet the criteria for the research projects listed in Article 31(10) of the Federal Statistics Act, including that the evaluators themselves meet the criteria to be considered as a scientific institution in Article 31(8). This legal basis has not yet been used to gain access to administrative data for ESF/ESF+ purposes[453]. Moreover, the difference may be visible in practice, as **access to certain databases within the same ministry may be easier**. For example, for the managing authority, access to data hosted by *Statistik Austria* is more

[450] Additional information provided by BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria).

[451] *Statistics Austria, Home Page*. https://www.statistik.at/en.

[452] *Bundesgesetz über die Bundesstatistik, (Bundesstatistikgesetz 2000), BGBl 4 . I, No. 163/1999, as amended by BGBl. I, No. 136/2001, BGBl. I, No. 71/2003, BGBl. I, No. 92/2007, BGBl. I, No. 125/2009, BGBl. I, No. 111/2010, BGBl. I, No. 40/2014, BGBl. I, No. 30/2018, BGBl. I, No. 32/2018, BGBl. I, No. 205/2021 and BGBl. I, No. 185/2022. https://www.statistik.at/fileadmin/pages/546/statistics_act.pdf.*

[453] Additional information provided by BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria).

cumbersome than access to data hosted by the Public Employment Service (AMS), as the latter is also part of the ministry, responsible for labour[454].

Box 28: Key findings – Legal obligations and conditions to access data in Austria

- The use of administrative data for ESF/ESF+ monitoring and evaluation is not specifically regulated by law and the Austrian DPA has not yet addressed this issue.
- The use of administrative data for ESF/ESF+ monitoring and evaluation is legitimised by the following legal provisions: (i) Article 44(1) CPR 2021 (formerly Article 54(1) CPR 2013); (ii) the legal bases for the processing of personal data in Article 6(1)(c) and (e) of the GDPR; and (iii) explicit consent if it is necessary to link special categories of personal data.
- Based on the provisions of the Research Organisation Act (*Forschungsorganisationsgesetz*), there are some differences in the legal obligations and conditions for access to data with regard to the purpose of data use. However, ESF/ESF+ evaluations do not qualify as scientific research, which means that evaluators cannot rely on the above-mentioned legal act.
- Although all types of actors could have access to administrative data for ESF/ESF+ monitoring or evaluation purposes, there may be differences depending on the body hosting the data. This is more of a practical issue, as access to administrative databases within the same public body is easier than access to data from other authorities, such as Statistics Austria.

6.2.3. Legal obligations and conditions to access data in Spain

Access to administrative data in Spain is mainly intended as **access to public data**, which is not only a procedure, but also **a right under the Spanish Constitution and legislation** (i.e., Law 39/2015[455] of 1 October on the Common Administrative Procedure of Public Administrations, as well as Law 19/2013[456] of 9 December on transparency, access to public information and good governance). Law 39/2015 covers *inter alia* the administrative procedures common to all public administrations and must therefore be considered when personal data are transmitted from one public authority to another for another purpose. Some examples of different models used at national level to access and link administrative data could arise from these different legislative acts.

The legal obligations and conditions for access to data are regulated by Articles 17 et seq. of Law 19/2013. There are no different rules for access to administrative data depending on

[454] Additional information provided by BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria).

[455] Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations, *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*. https://www.boe.es/eli/es/l/2015/10/01/39/con.

[456] Law 19/2013, of 9 December, on transparency, access to public information and good governance, *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*. https://www.boe.es/eli/es/l/2013/12/09/19/con.

specific factors such as the use of the data (evaluation vs. monitoring), the sector of the user (evaluator) requesting access to the data (academic, governmental, private, non-governmental), the age of the data subject (children vs. adults), the residency of the evaluators (local evaluators vs. foreign evaluators), or the hosting of the data (data hosted by the statistical office or another body).

Title I of Law 19/2013 regulates and increases the transparency of the activities of all subjects that provide public services or exercise administrative powers, through a set of provisions contained in two separate chapters and from a dual perspective: active disclosure and the right of access to public information. The subjective scope of application of this Title (Article 2) is very broad and includes all public administrations, autonomous bodies, state agencies, public business entities and public law entities, insofar as they have regulatory or control functions over a specific sector or activity, as well as public law entities with their own legal personality, linked to or dependent on one of the public administrations, including public universities.

Chapter III (Articles 12 - 24) of Law 19/2013 broadly configures the right of access to public information, which is held by all persons, and which may be exercised without the need to provide reasons for the request. Public information is understood to be any content or document, regardless of its format or medium, in possession of any of the subjects included in the scope of Chapter III and created or acquired in the exercise of their functions (Article 13). Article 14 of Law 19/2013 provides for a series of limitations to the right of access to information, which shall be applied in accordance with a harm test (of the interest to be protected by the limitation) and the public interest in disclosure (that in the specific case the public interest in disclosure of the information does not prevail), and in a manner that is proportionate and limited by its object and purpose. Thus, on the one hand, insofar as the information directly affects the organisation or public activity of the body, access prevails, while on the other hand, protection is granted to data that are classified as specially protected in the Organic Law 3/2018[457] of 5 December on Personal Data Protection and the guarantee of digital rights, and its implementing regulations, access to which generally requires the consent of the holder, as well as in the GDPR.

It should be noted that other regulations with a sectoral scope also provide for access to public information. This is the case, for example, of Law 37/2007 of 16 November on the reuse of public sector information, which regulates the use of documents held by public sector administrations and bodies. As mentioned in its preamble, Law 37/2007 has specific features that delimit it from the general regime of access provided for in Article 105 b) of the Spanish Constitution and in its legislative development, essentially represented by Law 30/1992, of 26 November, on the Legal Regime of the Public Administrations and Common Administrative Procedure.

It is foreseen that public sector administrations and bodies are the ones to **decide whether or not to authorise the reuse of documents or categories of documents held by them for commercial or non-commercial purposes** (Article 4 Law 37/2007). Furthermore, according to Article 4(6), the reuse of documents containing personal data is governed by the provisions of Organic Law 3/2018.

This cross-reference to Organic Law 3/2018 implies that **reuse is not automatic** when the right to protection of personal data is at stake, and that the public sector body cannot systematically invoke the need to comply with Law 37/2007 as a legitimate reason for providing this data. On the other hand, Law 37/2007[458] does not apply to documents in respect of which the right of access is prohibited or limited by the provisions of Law

[457] Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).

[458] Law 37/2007 of 16 November 2007 on the reuse of public sector information, *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público*. https://www.boe.es/eli/es/l/2007/11/16/37/con

19/2013[459], of 9 December, on transparency, access to public information and good governance and other regulations governing the right of access or registry publicity of a specific nature (Article 3.3.a).

According to the Spanish Data Protection Agency[460], the reuse of data by public administrations is widely known in Spanish legislation and Law 18/2015, of 9 July, which modifies Law 37/2007, of 16 November, on the reuse of public sector information, establishes that the administrations and public bodies have an unequivocal obligation to authorise the reuse of personal data, including those institutions in the cultural field such as museums, archives, and libraries. However, **the reuse of data for ESF/ESF+ purposes is not specifically regulated and hardly discussed**. There is no direct interaction between the Spanish Data Protection Agency (AEPD) and the Spanish managing authority (UAFSE).

Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations and the aforementioned law establish **the need for certain electronic tools** used by different public administrations to allow the exchange of information between them in an automatic and interoperable manner. Specifically, electronic relations between public administrations are regulated in Articles 155-158 of Chapter IV of Title III of Law 40/2015 of 1 October. Specifically, Article 155 regulates the transmission of data between public administrations and Article 156 defines the National Interoperability Scheme and the National Security Scheme. Article 157 regulates the reuse of systems and applications owned by the administration while Article 158 deals with the transfer of technology between administrations.

Article 155 of Law 40/2015[461], of 1 October, on the Legal Regime of the Public Sector, states that each administration must "*facilitate access by the other public administrations to the data relating to data subjects in their possession, specifying the conditions, protocols and functional or technical criteria necessary to access such data with the maximum guarantees of security, integrity and availability"*. This access must take place in compliance with the requirements and conditions established in the regulations on personal data, as well as any special regulations that may be applicable in each case and that may limit the possibility of using the data obtained from other entities.

Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of e-Government (*Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*), was repealed by Royal Decree 311/2022[462], of 3 May, regulating the National Security Scheme (*Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*). The National Security Scheme (ENS) is articulated with the aim of creating and implementing a security policy for the protection of data in the use of electronic media. For its development, it establishes the basic pillars and minimum requirements to guarantee that information benefits from a high level of protection. This regulation is addressed to public administrations, which are obliged to implement the ENS, as well as to all private entities that interact with public administrations under concession and provide them with services[463].

[459] Law 19/2013, of 9 December, on transparency, access to public information and good governance, *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*. https://www.boe.es/eli/es/l/2013/12/09/19/con

[460] Interview, Agencia Española de Protección de Datos, 18 October 2022.

[461] Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*. . Available at: https://www.boe.es/eli/es/l/2015/10/01/40/con.

[462] Royal Decree 311/2022 of 3 May, which regulates the National Security Scheme, *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*. Available at: https://www.boe.es/eli/es/rd/2022/05/03/311/con.

[463] See: https://adefinitivas.com/arbol-del-derecho/el-nuevo-esquema-nacional-de-seguridad-a-cargo-de-mar-ibanez/

Box 29: Key findings – Legal obligations and conditions to access data in Spain

- Although the reuse of data by public administrations is widely regulated in Spanish legislation, the Spanish Data Protection Agency believes that the reuse of data for ESF/ESF+ purposes is not specifically regulated and hardly discussed.
- In general, access to administrative data in Spain is mainly regulated by Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations, as well Law 19/2013, of 9 December, on transparency, access to public information and good governance. Other regulations with a sectoral scope may also provide for access to public information. The public sector administrations and bodies are the ones to decide whether or not to authorise the reuse of documents or categories of documents held by them for commercial or non-commercial purposes (Article 4 Law 37/2007). There are no specific rules for access to administrative data depending on specific factors such as the use of the data (evaluation vs. monitoring), the sector of the user (evaluator) requesting access to the data (academic, governmental, private, non-governmental), the age of the data subject (children vs. adults), the residency of the evaluators (local evaluators vs. foreign evaluators), or the hosting of the data (data hosted by the statistical office or another body).

6.2.4. Legal obligations and conditions to access data in Italy

In Italy, access to administrative data is mainly regulated by Chapter 5 (Articles 22 to 28) of Law 241/90[464] as well as by Presidential Decree No. 184/2006[465]. No different rules were found for access to administrative data depending on specific factors such as the use of the data (evaluation vs. monitoring), the sector of the user (evaluator) requesting access to the data (academic, governmental, private, non-governmental), the age of the data subject (children vs. adults), the residency of the evaluators (local evaluators vs. foreign evaluators), or the hosting of the data (data hosted by the statistical office or another body). It should be noted that the Italian DPA recently held that only national (and not regional) legislators were competent to legislate on the issue of the use of health data for research purposes[466].

Regarding the reuse of personal data for research purposes[467], Italy has introduced more restrictive measures, codifying in Articles 110 and 110-bis of the Italian Privacy Code[468] a

[464] Law No 241 of 7 August 1990, New rules on administrative procedure and the right of access to administrative documents., *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.* Available at: https://www.normattiva.it/eli/id/1990/08/18/090G0294/CONSOLIDATED/20230203.

[465] Presidential Decree No 184/2006. Available at: https://www.altalex.com/documents/leggi/2013/05/02/regolamento-sull-accesso-ai-documenti-amministrativi.

[466] See Opinion of the Garante, *Warning measure on treatments carried out in relation to the green certification for Covid-19 provided for by Law Decree No 52 of 22 April 2021*, 23 April 2021, available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9578184 p. 2 onwards (last accessed 13 March 2022), and *Warning measure to the Campania region regarding the use of the COVID-19 green certifications of 25 May 2021*, 25 May 2021, available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/9590466, p. 3 (last accessed 13 March 2022).

[467] *AboutPharma, Il riutilizzo dei dati personali a fini di ricerca anche alla luce dei più recenti orientamenti del Garante (The re-use of personal data for research purposes also in the light of the most recent guidelines of the Garante)*. https://www.aboutpharma.com/legal-regulatory/il-riutilizzo-dei-dati-personali-a-fini-di-ricerca-anche-alla-luce-dei-piu-recenti-orientamenti-del-garante/ Available at: https://www.aboutpharma.com/legal-regulatory/il-riutilizzo-dei-dati-personali-a-fini-di-ricerca-anche-alla-luce-dei-piu-recenti-orientamenti-del-garante/.

[468] Legislative Decree No 196 of 30 June 2003 - Personal Data Protection Code, containing provisions for the adaptation of the national system to Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and

system that bases the processing of data for scientific research purposes either on the consent of the data subject or, if this is not possible, on a series of procedural requirements, including the obligation of prior consultation with the Italian DPA, already provided for in Article 36 of the GDPR (or even prior authorisation, with the mechanism of silence-rejection). In particular, pursuant to Article 110 of the Privacy Code, the processing of data for scientific research purposes is possible in the absence of the consent of the data subject, if:

- the processing is carried out on the basis of legal provisions, regulations or under the GDPR (Article 9(2)(j)), and an impact assessment is conducted and made public (a situation that legitimises processing by public and private facilities on the basis of specific legal provisions).

- it is impossible to inform the data subjects or excessively burdensome, or risks jeopardising the purposes of the research, provided that (i) appropriate measures are taken to protect the rights and freedoms of the data subjects, (ii) the research programme is subject to a favourable opinion of the competent ethics committee, and (iii) the programme is subject to prior consultation of the Guarantor (Italian DPA) pursuant to Article 36 of the GDPR.

Similarly, the further processing of data may be authorised by the Guarantor, also by means of general measures, when there are the same reasons of impossibility or objective difficulty in contacting the data subjects, or the research activity may be prejudiced (Article 110-bis of the Privacy Code).

The Italian DPA has also published the 'DPO Handbook'[469], issued to guide and support DPOs in the public and semi-public sectors.

Legislative Decree 82/2005[470], also known as the Digital Administration Code (CAD), gathers and organises the provisions concerning the digitalisation of the public administration in its relations with citizens and companies. Article 50 CAD governs the availability of public administration data. Among the limitations that this Article places on the use and exploitation of public administration data, the rules on the protection of personal data are explicitly mentioned. Moreover, and also with specific reference to the communication of personal data between public administrations, Article 50(2) of the CAD makes it clear that compliance with the applicable data protection legislation is essential, even in cases where the transmission of data is necessary for the performance of the institutional tasks of the requesting administration (*"Any data processed by a public administration, with the exemptions referred to in Article 2(6), except in the cases provided for in Article 24 of Law No. 241 of 7 August 1990, and in compliance with the legislation on data protection, shall be made accessible and usable by other administrations when the use of the data is necessary for the performance of the institutional tasks of the requesting administration […]"*).

Therefore, the legislation on the processing of personal data, i.e. the GDPR and Legislative Decree 196/2003[471], prevails over the legislation on the communication of data between public administrations, which constitutes an explicit limitation.

repealing Directive 95/46/EC. (Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679) (Italy). https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig

[469] *The Italian DPA, 2019, Manuale RPD Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea (Regolamento (UE) 2016/679) (DPO Manual Guidelines for Data Protection Officers in the public and para-public sectors for compliance with the EU General Data Protection Regulation)*.

[470] Legislative Decree No 82/2005, *DECRETO LEGISLATIVO 7 marzo 2005, n. 82* (Digital Administration Code). https://www.normattiva.it/eli/id/2005/05/16/005G0104/CONSOLIDATED

[471] Legislative Decree No 196 of 30 June 2003, *DECRETO LEGISLATIVO 30 giugno 2003, n. 196* (Privacy Code). https://www.normattiva.it/eli/id/2003/07/29/003G0218/CONSOLIDATED.

Box 30: Key findings – Legal obligations and conditions to access data in Italy

- Access to data is mainly regulated by Law 241/90 and by Presidential Decree No. 184/2006.
- No rules were found for access to administrative data that would concern the use of the data (evaluation vs. monitoring), the sector of the user (evaluator) requesting access to the data (academic, governmental, private, non-governmental), the age of the data subject (children vs. adults), the residence of the evaluators (local evaluators vs. foreign evaluators) or the hosting of the data (data hosted by the statistical office or another body). However, the Italian DPA recently ruled that only national (and not regional) legislators are competent to legislate on the use of health data for research purposes.
- Although the Italian DPA is aware of the reuse of administrative data for ESF/ESF+ purposes, it has not issued any specific opinions or guidelines for this context. In its 2014 guidelines, the Italian DPA deals in general with the reuse of data. On the other hand, a DPO Handbook provides guidance to DPOs in the public and semi-public sector.
- Lastly, Legislative Decree 82/2005, also known as the Digital Administration Code (CAD), makes it clear that compliance with the applicable data protection legislation is essential, even in cases where the transmission of data is necessary for the performance of the institutional tasks of the requesting administration.

7. Conclusions and recommendations

The purpose of this study has been to assess the legal and practical challenges in accessing and reusing administrative data for the purpose of monitoring and evaluating the ESF and ESF+ programmes. To facilitate ESF+ monitoring and evaluation, the study has also assessed how to facilitate the access to administrative data with the aim of providing guidance to managing authorities on how to process personal data, including administrative data while complying with data protection rules.

To reach conclusions, the study has reviewed data protection and ESF+ relevant laws at an EU and national level in nine EU Member States: Austria, Germany, Spain, France, Ireland, Italy, Poland, Romania, and Sweden. In addition, 50 stakeholder interviews were conducted with a wide range of stakeholder types in these nine countries to identify practices, challenges, and possible solutions concerning data processing for the purpose of monitoring and evaluating the ESF and ESF+. Moreover, to ensure the formulation of robust and practical recommendations that combine the monitoring and evaluation needs of the ESF/ESF+ with the fundamental right to data protection, a Focus Group meeting with stakeholders from 13 EU Member States was organised.

Based on this work, the study first reported on the main conclusions of the stakeholder interviews. With regard to obtaining personal data on the ESF participants, the stakeholder interviews informed on how the systems differ in the nine Member States assessed in this study. The systems differ in terms of the degree of centralisation of data storage, the extent to which data are anonymised before being transmitted to the managing authority and/or evaluators, and the practices of how evaluators collect and/or access data (whether they collect them from managing authorities, central or regional databases and/or directly from ESF participants). The stakeholder interviews also informed the study on the degree of centralisation in the nine Member States concerning the processing of administrative data,

the challenges and solutions identified, and the extent to which stakeholders seek and use advice, for example from data protection authorities.

Second, the study examined the legal framework for personal data that is relevant for the ESF+ monitoring and evaluation (GDPR, CPR 2021 and ESF+ Regulation, including relevant national implementing or supplementing legislation). It also described in more detail the legal framework at EU level that has data protection implications for the monitoring and evaluation of the ESF+, including data protection relevant articles in the TFEU, the EU Charter, and the GDPR as well as the case law of the CJEU.

Third, the study provided an overview of the national legal frameworks to gain further insight into how a selection of nine Member States apply and complement the EU legal framework and found a diversity of legal practices. The study also provided examples of dataset- and sector-specific legislation from three selected Member States (Austria, Romania and Spain) to provide a deeper insight into the diversity and multiplicity of national legislation to be considered for each different type of public sector data. The examples illustrate that the answers to data protection requirements and questions in the case of monitoring and evaluation of ESF/ESF+ programmes are not straightforward and cannot be explained solely by interpreting EU data protection rules. The study argues that in order to address legal issues in accessing administrative data for monitoring and evaluation purposes, not only national GDPR implementing legislation and ESF/ESF+ implementing legislation should be examined, but also (pre-)existing national sectoral legislation and database-specific legislation, depending on the sector and type of data.

Fourth, the study analysed data protection aspects relevant for the monitoring and evaluation of ESF+, including the relevant legal bases, provisions and national practices relevant for data re-use, consent, special categories of personal data, data transmission, data linkage, data storage and information to data subjects. In particular, the analysis covers three Member States (Austria, Romania and Spain) that were selected for the in-depth review.

Although several legal bases in Article 6 GDPR could be used to legitimise the processing of personal data of participants and non-participants for ESF/ESF+ monitoring or evaluation, the study argues that the most appropriate legal bases seem to be (i) compliance with a legal obligation (Article 6(1)(c)) and (ii) performance of a task carried out in the public interest (Article 6(1)(e)). Both of these legal bases leave some discretion to Member States in a sense that national GDPR-implementing laws may contain specific provisions to adapt the application of the GDPR rules, as stated in Article 6(2) and (3) GDPR. A review of national laws in the three Member States showed that Romania used this option for letter (e), Spain for letters (c) and (e), and Austria did not use its discretion.

In addition to the legal basis, the study analysed data protection aspects relevant for the monitoring and evaluation of the ESF/ESF+ concerning the reuse of personal data, consent, special categories of personal data, transmission of data, data linking, data storage, and informing data subjects. This analysis showed that:

- There are interpretations and arguments both for considering that evaluations carried out or commissioned by the managing authorities are considered as scientific research and others against, partly deriving from the three criteria of a EDPS Preliminary opinion.

- National stakeholders usually rely on consent when collecting personal data directly from ESF/ESF+ project participants. However, if problems in the validity of consent occur, national authorities cannot migrate from consent to another legal basis retroactively in order to justify processing. Only in certain cases can consent be replaced with another legal basis, which better reflects the situation, i.e., in case of withdrawal of a consent or processing for a new/additional purpose. However, any

change must be notified to data subjects in accordance with the information requirements in Articles 13 and 14 GDPR.

- Relying on explicit consent to lift the prohibition to process special categories of personal data is especially challenging. Instead, it may be more suitable to use Article 9(2)(g) on the processing for reasons of substantial public interest, Article 9(2)(h) on the procesing for reasons of medicinal purposes or for example Article 9(2)(i) on the processing of data for reasons of public interest in the area of public health.

- Transmission of data falls under the definition of a processing operation, meaning that any transmission should comply with basic data protection principles in Article 5 GDPR. In the context of ESF+, the transmission of data is further governed by specific EU and national legislation.In order to conclude on the individual obligations of actors involved in transmissions of data for ESF+ purposes, specific national legislation thus needs to be examined.

- Although the GDPR does not use this term, 'data linking' falls under the GDPR definition of 'processing' of personal data in Article 4(2) GDPR and hence requires a clear legal basis.

Fifth, in reviewing national practices, the study identifies two different models for accessing and linking administrative data for ESF/ESF+ monitoring and evaluation – centralised and decentralised. Only Sweden is an example of having a centralised model of access to administrative data. Sweden has a centralised and harmonised model where access to administrative data for ESF/ESF+ purposes is centralised at Statistics Sweden. The other eight Member States (Germany, Spain, France, Ireland, Italy, Poland, Austria, and Romania) have, to different degrees, decentralised models. In these Member States, there may be central databases containing data collected directly from ESF/ESF+ participants. However, pre-existing administrative data used to complement and link data for monitoring and evaluation are neither coordinated nor processed centrally.

Finally, this chapter draws conclusions from the study, introduces the main challenges identified and develops recommendations to overcome them.

7.1. Main issues and challenges identified and recommendations to overcome them

These recommendations consider the results of the study including from the Focus Group and are designed to tackle the main issues and challenges identified in this study. There are 22 recommendations grouped into seven overall sub-sections. Each section provides background to the issue at stake, discusses the main challenges and proposes recommendations to tackle them.

7.1.1. Issues related to knowledge and choice of the most appropriate legal basis

The first challenge is that there are several possible legal bases for accessing administrative data for ESF/ESF+ monitoring and evaluation purposes and diverging interpretations of EU and national laws on the most appropriate legal basis. The processing of administrative data, including the processing of participant and non-participant data for ESF/ESF+ monitoring and evaluation purposes, and the new use of personal data from existing data

registers, may involve the processing of personal data. Therefore, all processing operations (such as access to administrative data) must comply with EU and Member State data protection rules, i.e., these processing operations must have a valid legal basis. However, it is difficult for managing authorities, beneficiaries, and evaluators to navigate between the possible legal bases and to assess which one is the most appropriate, effective, and efficient to use for data processing in the monitoring and evaluation of the ESF+.

Sources and case law at EU level show that although several legal bases in the GDPR[472] can be used to legitimise the processing of (including access to) administrative data of participants and non-participants for the ESF/ESF+ monitoring or evaluation, the most appropriate legal bases appear to be:

- fulfilment of a legal obligation[473] and
- the performance of a task carried out in the public interest[474].

These two legal bases provide Member States with the discretion to further regulate on certain aspects of data processing[475] in their national legislation. The use of consent as a legal basis has been the most common practice so far in the Member States sampled for this study when collecting personal data directly from ESF participants. However, the legal analysis in Section 5.3 shows that using consent as a legal basis is often not suitable, especially not when personal data are collected by a public authority. Moreover, collecting personal data using consent forms may create a heavy administrative burden due to difficulties related to obtaining consent and in case of its withdrawal. In such a case, it is challenging to migrate to another legal basis to facilitate the reuse of such data.

The 2021 Common Provisions Regulation (CPR 2021)[476] further allows Member States to process personal data in order to fulfil their obligations under the Regulation, including for the monitoring and evaluation of the ESF+, as long as the personal data is processed in accordance with the GDPR. In addition, the ESF+ Regulation[477] stipulates that Member States may enable managing authorities to process personal data from national administrative registers for new purposes, in accordance with the GDPR legal bases concerning processing that is necessary to comply with a legal obligation (Article 6(1)(c) GDPR) or to perform a task carried out in the public interest (Article 6(1)(e) GDPR). These two legal bases leave Member States with some discretion on certain aspects of data processing, as defined in Article 6(2) and (3) GDPR. A review of national laws in the three Member States showed that Romania made use of the option to further legislate in the case of legal basis in Article 6(1)(e) GDPR – public interest, while Spain uses the option to further legislate also in the case of legal basis in Article 6(1)(c) GDPR – legal obligation. Austria did not decide to use the option to further legislate.

Ambiguity in the choice of legal basis was also visible from stakeholder responses. While in most Member States consent was the main legal basis for the collection of personal data from participants, no conclusive information on the legal basis for accessing administrative data could be obtained. For instance, one beneficiary in Sweden, the Public Employment Service, explained that as a public institution, the use of explicit concent as a legal basis is legally questionable, and uses instead its legal obligation as a legal basis. During the Focus Grouo meeting, the Romanian managing authority stated that it wanted to use the public

[472] Article 6, GDPR.

[473] Article 6(1)(c), GDPR.

[474] Article 6(1)(e), GDPR.

[475] Articles 6(2) and (3), GDPR.

[476] Article 4, CPR 2021.

[477] Article 17(6), ESF+ Regulation.

interest as a legal basis to process administrative data, but that the national DPA advised against it.

In order to address the issue of diverging interpretations of the most appropriate legal basis, this study recommends that guidance be provided at national and EU level taking into account specific national circumstances.The following **recommendations** are proposed:

1. Member States and/or managing authorities should ensure that legal advice or guidance on applicable data protection rules, including the legal basis for processing, is sought from the national DPA or data protection officers. If a legal opinion would reveal gaps in thelegal framework, Member States should consider possible legislative initiatives to provide a clear legal basis, and/or to formulate clear national provisions governing other aspects of the processing of personal data for ESF+ evaluation and monitoring, in accordance with the GDPR .

2. In addition, where the existing legal framework is considered sufficient and clear enough, Member States and/or their administrative authorities should invest in providing clear guidance on applicable data protection rules. These guidelines should provide examples of good practice among national stakeholders.

The measures described above would facilitate data processing by ESF+ beneficiaries, evaluators and other national actors who need to access administrative data while complying with the EU and national data protection legal framework.

Moreover, interventions during the Focus Group suggested that guidance for all Member States would be welcome. The Focus Group participants recommended that the Commission provides guidance on the legal basis in the GDPR and how it may be used to access personal data from administrative registers for the purpose of monitoring and evaluating the ESF+.

Box 31: Recommendations – Provide guidance and obligations at national level to avoid ambiguity in the choice of legal basis

- Member States and ESF+ managing authorities should consult their national DPA on the applicable data protection rules, including the legal basis for processing personal data for the purpose of ESF+ evaluation and monitoring, if there is any doubt regarding the available options under national or Union law.

- Where a gap in legislation is identified, Member States should consider possible legislative initiatives to provide clear data protection rules, including a legal basis for reusing administrative data for the purpose of ESF+ monitoring and evaluation.

7.1.2. Challenges related to the reuse of administrative data and/or the further use of data for scientific research

The reuse of data from existing administrative datasets is not always possible due to concerns of lack of clear rules allowing such use or the existing lack of knowledge of applicable rules when such exist.

In the context of ESF+ monitoring and evaluation, the main reasons for reusing data are:

- in the case of counterfactual evaluations, where access to data of a control group (non-participants) is needed;

- in the case of data on individual programme participants, to avoid the inefficiency of collecting information that already exists in national registers; and

- to avoid asking sensitive questions to participants.

The reuse of data refers to two situations: (i) where data originally collected for purposes other than participation in ESF+ projects are reused on the basis of a new legal basis, and (ii) where data collected are used for additional/further purposes but still based on the same legal basis.

The purpose limitation principle[478] prohibits the further use of data for another purpose incompatible with the original purpose for which the data were collected. This means that administrative data in existing national databases can only be further processed for ESF+ monitoring and evaluation purposes if the necessary conditions are met (e.g., if such a further use is compatible with the original purpose, including the case where processing for ESF+ purposes could be considered as scientific research). In the case of evaluations, there are arguments both for considering that evaluations carried out or commissioned by the managing authorities can be considered as scientific research and for considering that they cannot, also depending on the scope and quality of the methodology of the evaluations in question.

In this study, stakeholder interviews revealed that there are examples of access to administrative data in all Member States that were selected in this study. Types of actors identified that have access to these data mainly include evaluators. In Italy and Sweden, interviews indicated that managing authorities can also access these data, and in Romania and Sweden also beneficiaries. In Ireland, while the managing authority has not had access to administrative data, intermediary bodies have. However, according to interviewees, these actors seem to be able to access administrative data only in an anonymised form. This means that data is transmitted in a form that does not allow the identification of a data subject. Furthermore, in some countries, such as Ireland, respondents indicated that data from administrative registers could only be accessed, transferred or reused if data sharing agreements and data protection impact assessments (DPIA) were in place.

In order to enable reuse of administrative data and further processing for scientific research, the following **recommendations** are proposed:

3. Given their obligation under the CPR and ESF+ Regulationto evaluate and monitor ESF+, Member States should consider determining in their national legislation the legal basis for the reuse of data in their administrative registers when such data is used for ESF+ evaluation and monitoring purposes. In particular, they should determine the legal obligation (in accordance with Article 6(1)(c) GDPR) or a task carried out in the public interest (in accordance with Article 6(1)(e) GDPR) which necessitates the processing of personal data.

4. If there is no legal basis for the reuse of administrative data in national law, it is necessary to demonstrate that the purpose of reusing administrative data is compatible with the initial purpose of processing these administrative data, except if the reuse is carried out for the purpose of scientific research and evaluations can be considered to qualify as such research[479]. In some Member States such as Austria, evaluations are not considered to be scientific research.

[478] Article 5(1)(b), GDPR.

[479] GDPR, Article 5(1)(b) in connection with Article 89(1).

5. According to its work programme 2023-2024, the EDPB is currently working on guidelines on data processing and scientific research which could also further clarify the GDPR concept of 'scientific research purpose'.

6. In the meanwhile, in order to clarify the definition of scientific research and its application in the context of the ESF+ and taking into account the specific circumstances of each Member State, managing authorities or other national stakeholders could also seek advice from their national DPAs. For example, upon request, national DPAs could facilitate data processing by providing opinions and/or guidelines, taking into account the following questions:

   - Can the processing of certain administrative data for ESF+ monitoring and evaluation purposes be considered compatible with the initial purpose of data collection?

   - Can the processing of certain administrative data for ESF+ evaluation purposes be considered as scientific research and therefore compatible with the initial purpose?

   - What conditions should be fulfilled for such processing to fall under the category of scientific research?

   - What safeguards should be provided to data subjects in the case of scientific research (see Article 89(1) GDPR)?

   Member States and/or managing authorities would need to inform the relevant national stakeholders of the possibility to rely on such compatible purposes or scientific research and ensure that such advice is understood. Beneficiaries, evaluators and other national stakeholders accessing administrative data would then have to comply with such a legal opinion and/or guidance.

7. At a more practical level, access to administrative data could be facilitated through data sharing agreements. In order to initiate such agreements, the managing authority should, in dialogue with the administrative data holders and the stakeholders who need to access the data, clarify the need and the legal possibilities to conclude such agreements. This would potentially facilitate access to administrative data, e.g. for evaluators, as such an agreement could reduce the administrative burden and legal complexity for individual parties seeking access to administrative data on an *ad hoc* basis.

Box 32: Recommendations – Faciliate the reuse of administrative data and/or clarify the definition of scientific research

- Member States should provide a clear legal basis for the reuse of administrative data at national level.

- National DPAs should provide opinions/guidelines on when the reuse of administrative data can be considered as processing for 'compatible purposes', on the possibility to further process personal data for scientific research purposes, when ESF+ evaluation can be considered as 'scientific research', as well as on the appropriate safeguards for data subjects.

- National administrative authorities should conclude data sharing agreements to facilitate the exchange of administrative data for ESF+ purposes.

7.1.3. Challenges related to the processing of special categories of personal data

The processing of special categories of personal data requires both a valid legal basis and an exemption to lift the prohibition on the processing of special categories of personal data. As the processing of special categories of personal data represents a greater interference with the rights of data subjects, the GDPR requires that specific safeguards are provided by law to protect individuals' personal data.

Stakeholder interviews showed that for the ESF 2014-2020 programming period, beneficiaries in most of the Member States covered by this study collected special categories of personal data. However, in some Member States it was not always possible to process special categories of personal data. Respondents from Ireland and Italy indicated that these data could not be reused, and in Germany one respondent mentioned that there were restrictions on collecting these data and prohibitions on making informed estimates. In Spain, several interviewees reported that there are difficulties in collecting these data.

The study therefore proposes the following **recommendations**:

8. Beneficiaries and other national actors processing personal data should consider to what extent it is necessary to process special categories of personal data and whether it is possible to use anonymised data instead ('data minimisation').

9. If it is necessary to process special categories of personal data and anonymisation of such data is not an option, stakeholders need to ensure that any processing of such data has a legal basis under Article 6(1) GDPR and an applicable exemption to lift the ban on the processing of such data, including the necessary safeguards (Article 9(2) GDPR).

10. In addition, stakeholders should ensure that suitable and specific measures to safeguard data subject's rights are in place, as required by national law on the basis of the GDPR (Article 9(2) GDPR), for example through the use of pseudonymisation. The completion of a DPIA could help to identify and mitigate such risks.

11. In case of ambiguity in identifying the applicable legal provisions allowing the processing of special categories of personal data, it is recommended that Member States and/or managing authorities seek advice from their national DPAs, which would thus have to issue a legal opinion or guidelines to be followed by national stakeholders when processing special categories of personal data for ESF+ purposes. It is recommended that the national stakeholders also seek advice from data protection experts, such as their DPOs or consultants, as appropriate.

12. Althought the alternative was assessed as irrelevant by most of the participants of the Focus Group of this study, it is advised that beneficiaries should make use of informed estimates when reporting on indicators that could involve the processing of special categories of personal data. As some methods of informed estimates still rely on data collected from participants (e.g., sampling approaches method), methods that do not require collection of individual data should be prioritised (e.g., methods based on proxies and educated guesses).

Box 33: Recommendations – Facilitate the processing of special categories of personal data

- When processing special categories of personal data, apply the principle of data minimisation, including through anonymisation.
- Ensure that there is a legal basis for the processing as well as an applicable exemption to lift the prohibition to process special categories of personal data and that the appropriate safeguards required by national law are in place.
- If necessary, seek advice on applicable rules and appropriate safeguards from data protection experts (national DPAs, DPOs, or consultants).
- Use of alternative methods to process special categories of personal data (e.g., informed estimates).

7.1.4. Lack of understanding and/or awareness of the national legal framework for the processing of administrative data

To understand how personal data should be processed in Member States, several pieces of legislation need to be taken into account. The EU Charter and the ECHR must be respected, and any processing activity must also comply with the provisions of the GDPR, the CPR 2021 and the ESF+ Regulation.

In addition, national legislation must also be complied with, and here, too, several layers of instruments must be taken into account. The processing of personal data must comply with the requirements of national constitutions, national legislation supplementing the GDPR, national (or even regional) sectoral and dataset-specific legislation, as well as sector-specific data soft law. While general rules are set out in overarching legal instruments such as the GDPR, these do not always provide detailed rules on how to deal with each specific type of data, and therefore often allow Member States to adapt these rules or provide for more specific rules in light of the needs of processing operations in specific sectors. Certain legal bases of the GDPR[480] leave Member States the discretion to further regulate certain aspects of data processing in their national legislation. In the absence of clear guidance, actors involved in the monitoring and evaluation of the ESF+ may therefore face difficulties in understanding which rules apply and what possibilities they may entail.

Examples from the desk research and interviews conducted as part of this study illustrate a variety of requirements placed on personal data processing by national law:

- In Austria, the obligation of a managing authority to report certain data on the ethnicity of participants conflicts with the participants' fundamental freedom of confession of participants, based on which no person is obliged to reveal his or her ethnicity. This means that in Austria the processing of ethnicity data requires the consent of the individual.

[480] Article 6(1)(c) and (e), GDPR.

- The Spanish law[481] that complements the GDPR stipulates that a legal obligation and/or the task carried out in the public interest, or the exercise of official authority vested in the controller, should be set out in a norm with the force of law. As a result, a legal basis needed in Spain must be established in primary legislation, which cannot give the public body discretion to decide on the scope of its public interest task[482].

- In Romania, the supplementary law to the GDPR requires additional national legislation to legitimise certain processing operations. In addition, the national DPA stated that a protocol or similar document signed between two national bodies that are administrative data holders cannot constitute a legal basis for data processing and that the legal basis should be provided by law.

The different national legal frameworks result in different national/regional approaches to access to administrative data in practice. For example, interviews with stakeholders show that in some countries challenges related to access to administrative data have been overcome by updating legislation to allow the use of specific datasets and through data sharing agreements (Poland), by conducting a DPIA and by a continuous dialogue with the DPA (Italy) or by providing detailed guidelines for the reuse of administrative data (Spain).

To this end the following **recommendations** are proposed:

13. As the legal bases in Article 6(1)(c) and (e) of the GDPR require establishing a legal obligation or a task in the public interest Member States and/or managing authorities should seek advice from their national DPAs, which could issue a legal opinion or guidance to be followed by stakeholders accessing administrative data. It is recommended that the same stakeholders seek advice from data protection experts, such as DPOs or consultants, as appropriate. Beneficiaries, evaluators, and other actors accessing administrative data would need to ensure compliance.

14. In order to have a clearer understanding of the risks associated with the processing of administrative data in a specific situation, it is recommended to prepare a DPIA prior to the envisaged processing of data. While the GDPR only requires DPIAs in situations of possible high-risk processing (Article 35 GDPR), and there may be differences between Member States in the type of processing that warrant a DPIA, it is considered good practice to carry out a DPIA, in particular when processing is based on Article 6(1)(c) or (e) (especially if such a DPIA has not yet been carried out as a part of the general impact assessment in the context of the adoption of such legal bases). The DPIA should be developed by national actors who access and use personal data from national registers (i.e., data controllers). In order to assist controllers in carrying out DPIAs, managing authorities may develop templates for such assessments based on templates and guidance provided by their national DPAs. The exchange of promising examples of such DPIAs among national stakeholders could also be encouraged.

[481] Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).

[482] Judgment 292/2000 of 30 November 2000, BOE [Official Gazette] number 4, of 04 January 2001 (Constitutional Court). https://hj.tribunalconstitucional.es/HJ/en/Resolucion/Show/4276.

Box 34: Recommendations – Raise the awareness of national rules on the processing of administrative data

- Consider the possibilities, rather than limitations, provided by national legislation in combination with EU law to facilitate the processing of administrative data in an the ESF+ context.
- Seek advice, guidance, and/or participate in the training of data protection experts (national DPAs, DPOs, or consultants), where appropriate together with other data protection specialists, in order to better understand the applicable legal framework and requirements that apply to the processing of administrative data for the purpose of monitoring and evaluation of the ESF+.
- Carry out, where appropriate, DPIAs for new projects and encourage the exchange of promising examples or templates for such assessments.

7.1.5. Low levels of interoperability of national registers and challenges related to decentralised data processing

A common challenge in accessing administrative data is that the data relevant for ESF/ESF+ monitoring or evaluation are held by different institutions and/or at different administrative levels. These data may in some cases be hard to compare, also with ESF+ indicators, partly due to varying definitions of data. Thus, decentralised hosting of data may lead to issues related to the interoperability of national registers that are relevant for monitoring or evaluating the ESF+. In addition, different data sets may be subject to different data protection rules and different consent requirements. An example of centralised data processing is Sweden, where Statistics Sweden hosts and processes administrative data on behalf of the managing authority.

In order to overcome these challenges, this study makes the following **recommendations**:

15. Member States, managing authorities and/or other public authorities, including administrative data holders, should jointly, or through a single actor, start the process of centralising data processing, including data hosting. This would benefit managing authorities and evaluators, including external evaluators, by facilitating the processing of and access to both data collected from ESF+ participants and administrative data.

16. As an alternative solution to centralising data processing, including data hosting, Member States should consider improving the central coordination of access to administrative data for the purposes of ESF+ monitoring and evaluation. Such coordination of responsibilities could be given to a national managing authority or the national statistical institute to reduce the administrative burden for all actors seeking access to administrative data.

17. Partly as a solution to facilitate centralised data processing or centralised coordination to access data, this study recommends that the authorities involved use pseudonymisation techniques and communicate among themselves with the help of unique identifiers. Although pseudonomysed data are still considered personal data, a pseudonymisation technique can mitigate data protection risks. It involves the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information – unique identifier, provided that such additional information is stored

separately, and that technical and organisational measures are taken to ensure the confidentiality and integrity of the data. However, pseudonymisation can be complex and expensive, and it may be difficult to link pseudonymised data due to the lack of unique identifiers. Therefore, this recommendation may need to be implemented in conjunction with recommendations 20-22 in order to work out how to use the technique effectively in practice.

Box 35: Recommendations – Centralise and coordinate data processing and facilitate data processing

- Consider the possibility to centralise data processing, including the hosting of data relevant for the monitoring and evaluation of the ESF+.
- Promote the centralisation of the management and coordination of access to administrative data for the purposes of ESF+ monitoring and evaluation.
- Consider the use of pseudonymisation as a technique to mitigate data protection risks.

7.1.6. Challenges associated with unnecessary costs, delays and data incompatibility

Obtaining access to administrative data can be time-consuming and there may be a long waiting period after a request has been made (mentioned by respondents in Austria, Ireland, Poland, Spain and Sweden). There may also be financial costs associated with accessing administrative data, as organisations, especially external evaluators, may need to purchase data from data holders (challenges due to costs were mentioned by respondents in Austria, Poland, Romania and Sweden). In addition, data may be defined differently by data holders and data may not be comparable.

These challenges could be addressed by the following **recommendations**:

18. Sufficient planning may be required to ensure data availability and comparability, and to ensure that all legal requirements regarding data protection are met. Moreover, if the planning does not include a confidentiality threshold[483] sufficient to access the necessary data, time may be lost in redesigning the evaluation methodology.

19. Each actor involved in ESF+ monitoring and evaluation should therefore plan well in advance what data will be needed. The managing authority can coordinate planning with administrative data holders who may know what data are available. However, the planning and coordination process can be challenging, as discussed in the Focus Group meeting. For evaluation purposes, it can be a challenge for the managing authority to plan and coordinate access to administrative data in advance, as several steps are needed to clarify in detail which data are needed and from what period. Public procurement rules may also prevent managing authorities from coordinating with external evaluators in advance of an evaluation.

[483] A confidentiality threshold refers to a minimum amount of data subjects included in a data set that can ensure the anonymity of each data subject.

Box 36: Recommendations – Plan access to administrative data well in advance.

- Plan well in advance what administrative data will be needed to complement or replace direct data collection for ESF+ monitoring and evaluation.
- Managing authorities to coordinate planning with administrative data holders who may know what data are available.

7.1.7. Lack of mutual learning between Member States on data protection-related issues concerning access to administrative data for ESF/ESF+ purposes

There are practices that can be applied to overcome the challenges of accessing administrative data. Illustrative examples of good practice in accessing administrative data for ESF+ monitoring and evaluation purposes identified during the interviews in this study include the following:

- As reported in Section 6.1.1, in Sweden, the processing of administrative data for ESF/ESF+ purposes is managed centrally by SCB. This institution can link different datasets and ESF+ monitoring data through a unique identifier. This centralised system reduces the need to collect data directly from participants and increases the reliability of data and the efficiency of data processing.
- In Ireland, the JLD, which brings togetherpayment and administrative data from a number of authorities, enhances the ability to access and reuse administrative data for monitoring and evaluation purposes. More information can be found in Sections 3.2 and 6.1.1.
- In Austria, the process of transmitting administrative data for ESF evaluation purposes is managed centrally by the managing authority BMAW. For evaluations and impact analyses, evaluators have to request data through the BMAW, after pseudonymisation carried out by an external service provider. Such coordination efforts can facilitate planning and ultimately access to administrative data.
- In Poland, the TERYT database/register is used for monitoring purposes. This is the official register of the territorial division of Poland, maintained by the Central Statistical Office. It is a defined database from which the downloaded data categories will be selected at a later stage to complete the data of the ESF+ project participants.
- As reported in Section 6.1.4, in the Veneto region of Italy, the Veneto Lavoro system makes basic data collected by the Veneto Employment Centres available to researchers and research bodies through the public use file called ‘Mercurio’, from which researchers, universities, and research institutes can request access to administrative data.
- The French Data Protection Authority (CNIL) has documented several useful guidelines on its website, including a practical guide to the publication and reuse of data. For more information, see Annex III – Interview country summaries.

With this in mind, the following is **recommended**:

20. Member States should exchange good practices with their counterparts in other Member States, which would have an impact on both Member States and managing authorities.

21. In parallel, the European Commission, DG EMPL, should continue to invest in the organisation of contact points where relevant stakeholders from Member States can meet and network. Potential topics for such events could also include the mapping and discussion of possible good practices at Member State level.

22. The development of a practical document and/or handbook for Member States and/or competent authorities could be encouraged. This tool could present specific situations that have been identified as bottlenecks in accessing administrative data for ESF+ in certain Member States and provide practical examples of how best to address such situations. This would help Member States, managing authorities and other national stakeholders.

Box 37: Recommendations – Promote the exchange of good practices

- Promote the exchange of good practices between Member States on access to administrative data for ESF/ESF+ purposes.
- Continue to organise contact points where relevant stakeholders from Member States can meet and network. When relevant, involve DPAs in such fora.
- Promotion of the development of a practical document and/or handbook for Member States and/or competent authorities.

8. Annexes

8.1. Annex I – References

AboutPharma, Il riutilizzo dei dati personali a fini di ricerca anche alla luce dei più recenti orientamenti del Garante (The re-use of personal data for research purposes also in the light of the most recent guidelines of the Garante). https://www.aboutpharma.com/legal-regulatory/il-riutilizzo-dei-dati-personali-a-fini-di-ricerca-anche-alla-luce-dei-piu-recenti-orientamenti-del-garante/

Act (2007:459) on Structural Funds Partnerships (Lag (2007:459) om strukturfondspartnerskap) (Sweden), (2007). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2007459-om-strukturfondspartnerskap_sfs-2007-459

Act (2018:218) containing provisions supplementing the EU Data Protection Regulation (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning) (Sweden). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218

Act of 10 May 2018 on the Protection of Personal Data (Ustawa z 10 maja 2018 o ochronie danych osobowych). https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000

Act of 11 July 2014 concerning rules of implementation of programmes supported from Cohesion Policy in the financial period 2021-2027 (Ustawa z dnia 11 lipca 2014 o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020) (Poland).

Act of 28 April 2022 on the rules for the implementation of cohesion policy programmes financed in the financial perspective 2021-2027 (Ustawa z dnia 28 kwietnia 2022 o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2021-2027) (Poland).

Agencia Española de Protección de Datos (AEPD), Administraciones Públicas. https://www.aepd.es/es/areas-de-actuacion/administraciones-publicas

Agencia Española de Protección de Datos (AEPD), Publicaciones y resoluciones. https://www.aepd.es/en/publicaciones-y-resoluciones

Agencia Española de Protección de Datos (AEPD). Procedimiento Nº: AP/00023/2017

Austrian Institute for Economic Research, Das Operationelle Programm "Beschäftigung Österreich 2014 bis 2020" des Europäischen Sozialfonds, Endbericht der begleitenden Evaluierung, March 2022, pp. 156-157.

Ben Faiza v. France, CE:ECHR:2018:0208JUD003144612 (European Court of Human Rights, Judgment (Fifth Section) of 8 February 2018).

Benedik v Slovenia, CE:ECHR:2018:0424JUD006235714 (European Court of Human Rights, Judgment (Fourth Section) of 24 April 2018).

Bird&Bird. *GDPR Tracker - Special rules for special categories of data*. Retrieved 12 October 2022 from https://www.twobirds.com/en/capabilities/practices/privacy-and-data-protection/general-data-protection-regulation/gdpr-tracker/special-categories-of-personal-data

Bodil Lindqvist v Sweden, ECLI:EU:C:2003:596. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101

Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation (Forschungsorganisationsgesetz – FOG) StF: BGBl. Nr. 341/1981 idF BGBl. Nr. 448/1981 (DFB) (NR: GP XV RV 214 AB 778 S. 81. BR: S. 413.) (Federal law on general matters according to Art. 89 GDPR and the research organization (Research Organization Act – FOG)). https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009514

Bundesgesetz über die Bundesstatistik, (Bundesstatistikgesetz 2000), BGBl 4 . I, No. 163/1999, as amended by BGBl. I, No. 136/2001, BGBl. I, No. 71/2003, BGBl. I, No. 92/2007, BGBl. I, No. 125/2009, BGBl. I, No. 111/2010, BGBl. I, No. 40/2014, BGBl. I, No. 30/2018, BGBl. I, No. 32/2018, BGBl. I, No. 205/2021 and BGBl. I, No. 185/2022. https://www.statistik.at/fileadmin/pages/546/statistics_act.pdf

Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG) StF: BGBl. I Nr. 10/2004 (NR: GP XXII RV 252 AB 382 S. 46. BR: 6959 AB 6961 S. 705.), RIS - E-Government-Gesetz - Bundesrecht konsolidiert, Fassung vom 11.04.2023 (bka.gv.at).

C-175/20, SIA 'SS' v Valsts ieņēmumu dienests, EU:C:2022:124 (Court of Justice of the European Union (Fifth Chamber) of 24 February 2022). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62020CJ0175

Charter of Fundamental Rights of the European Union, (2012).

Circular 08/2015 National Eligibility Rules For Expenditure Co-Financed By The European Regional Development Fund (ERDF) Under Ireland's Partnership Agreement 2014-2020 (Ireland).

Circular 13/2015 Management and control procedures for the European Structural and Investment Funds Programmes 2014-2020 (Ireland).

Coesione Italia, Sistema Nazionale di Monitoraggio. https://opencoesione.gov.it/it/sistema_monitoraggio/

Collective Labour Relations Act (Austria).

Commission Delegated Regulation (EU) No 480/2014 of 3 March 2014 supplementing Regulation (EU) No 1303/2013 of the European Parliament and of the Council laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund, OJ L 138, 13.5.2014, p. 5–44. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0480

Costello-Roberts v. the United Kingdom,, CE:ECHR:1993:0325JUD001313487 (European Court of Human Rights, Judgment (Chamber) of 25 March 1993).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), (1981).

COVID tracing apps, E/03346/2020, (2020a). https://www.aepd.es/es/documento/e-03346-2020.pdf

Data Protection Act 2018 (Ireland). https://revisedacts.lawreform.ie/eli/2018/act/7/revised/en/html

Data Protection Implications of Contact Tracing Apps, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 16 August 2020). https://www.dsb.gv.at/download-links/dokumente.html

Data Protection Working Party. (2011). Opinion 15/2011 on the definition of consent. In.
Data Protection Working Party. (2013). *Opinion 03/2013 on purpose limitation*.

Data Protection Working Party. (2014). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*.

Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/622227/en

Data Sharing and Governance Act 2019 (Ireland).

Decision DSB-D213.1020, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 16 August 2020). https://www.dsb.gv.at/download-links/dokumente.html

Decision no. 2216 of 02 June 2020, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

Decision no. 2752 of 23 June 2020, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

Decision no. 2804 of 12 May 2021, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

Decision no. 2952 of 18 May 2021, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

Decision no. 6460 of 02 December 2020, (Înalta Curte De Casaţie Şi Justiţie, Secţia de Contencios Administrativ şi Fiscal (High Court of Cassation and Justice, Department of Administrative and Fiscal Litigation)).

Decision of 19 November 2020, GZ: 2020-0.743.659 (Vienna Contact Tracing Regulation), (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority)). https://www.dsb.gv.at/download-links/dokumente.html

Decision of the Constitutional Court, 15 June 2007, VfSlg. 18.146/2007. https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vfgh&Sammlungsnummer=181

46&SkipToDocumentPage=True&SucheNachRechtssatz=False&SucheNachText=True&ResultFunctionToken=e9c97a3e-8d9d-4e7a-a34e-429b1611f4be&Dokumentnummer=JFT_09929385_06G00147_00

Decision of the Federal Administrative Court, 18 December 2020, W256 2235360-1/5E. https://gdprhub.eu/index.php?title=BVwG_-_W256_2235360-1

Decree-law No. 139 of 8 October 2021 (Decreto-legge 8 ottobre 2021, n. 139) (Italy). https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2021-12-07&atto.codiceRedazionale=21A07259&elenco30giorni=true

Decree n°2016-126 of 8 February 2016 on the implementation of programmes co-financed by the European structural and investment funds for the period 2014-2020 - France (Décret n°2016-126 du 8 février 2016 relatif à la mise en œuvre des programmes cofinancés par les fonds européens structurels et d'investissement pour la période 2014-2020), (2016). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032000333

Decision No 23/2012 regarding the establishment of cases in which it is not necessary to notify the processing of personal data (Decizia Nr.23 din 26.03.2012 privind stabilirea cazurilor în care nu este necesară notificarea prelucrării unor date cu caracter personal) (Romania). http://www.legex.ro/Decizia-23-2012-119333.aspx

Definitions of the common ESF+ (and JTF) indicators (output and result indicators) of the programme period 2021-2027 (Definitionen der gemeinsamen ESF+ (und JTF) Indikatoren (Output- und Ergebnisindikatoren) der Programmperiode 2021-2027) (Austria).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (1995).

DPA's Opinion on Draft Law Draft law for a Federal Act amending the E-Government Act and the Passport Act 1992 (Implementation E-ID), (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 02 October 2020).

DPA's Opinion on Federal draft law amending the 1992 Student Support Act (StudFG Novelle), GZ: D055.654 2022-0.308.733 (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority)).

DPA's Opinion on the draft Federal Act amending the Federal Statistics Act 2000 and the Research Organisation Act, GZ: D055.518 2021-0.474.423 (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 03 August 2021).

ESF+ Data Support Centre. *Note on Informed Estimates, July 2020 (revised version)*.

ESF+ Programme Employment Austria & JTF 2021-2027 - Austria (ESF+ Programm Beschäftigung Österreich & JTF 2021-2027), (2021).

European Commission. *Why do we need the Charter?* Retrieved 12 October 2022 from https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en#:~:text=The%20Charter%20strengthens%20the%20protection,and%20freedoms%20in%20the%20Charter.

European Commission. (2018a). *Ethics and data protection*.

European Commission. (2018b). *Study on the monitoring and evaluation systems of the ESF: Final report*.

European Commission. (2019a). *Pilot and feasibility study on the sustainability and effectiveness of results for European Social Fund participants using counterfactual impact evaluations : final report*. https://data.europa.eu/doi/10.2767/39339

European Commission. (2019b). *Pilot and feasibility study on the sustainability and effectiveness of results for European Social Fund participants using counterfactual impact evaluations: Final report*.

European Commission. (2021). *Design and commissioning of counterfactual impact evaluations : a practical guidance for ESF managing authorities*. https://data.europa.eu/doi/10.2767/02762

European Court of Human Rights. (2022). *Guide to the Case-law of the European Court of Human Rights - Data protection*.

European Data Protection Board. (2019a). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0*.

European Data Protection Board. (2019b). *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)*.

European Data Protection Board. (2019c). *Opinion 3/2019 concerning theQuestions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))*. https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en

European Data Protection Board. (2020a). *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*.

European Data Protection Board. (2020b). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*.

European Data Protection Board. (2020c). *Guidelines 05/2020 on consent under Regulation 2016/679*.

European Data Protection Board. (2021). *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf

European Data Protection Supervisor. (2014). *Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the "Risk analysis for fraud prevention and detection in the management of ESF and ERDF" - ARACHNE*. https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check/risk-analysis-fraud-prevention-and_en

European Data Protection Supervisor. (2020). *A Preliminary Opinion on data protection and scientific research*. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

Federal Act concerning the Protection of Personal Data (DSG) (Bundesgesetz über den Schutz personenbezogener Daten) (Austria). https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html

Federal Act of 7 July 1976 on the Legal Status of Ethnic Groups in Austria (Ethnic Groups Act) (Volksgruppengesetz). https://www.jusline.at/gesetz/vgg/gesamt

Federal Chancellery. Inquiry on the Definition of the Term "Minority" in Austria, Statement (Bundeskanzleramt, Anfrage zur Definition des Begriffes "Minderheit" in Österreich) Nr. 2021-0.802.012, from 26 November 2021.

Federal law on the social insurance institution for the self-employed (Self-Employed Social Insurance Act) (Selbständigen-Sozialversicherungsgesetz) (Austria), (2018).

Framework Convention for the Protection of National Minorities. https://www.coe.int/en/web/conventions/cets-number-/-abridged-title-known?module=treaty-detail&treatynum=157

Federal Ministry of Digitisation and Economic Location (Bundesministerium Digitalisierung und Wirtschaftsstandort), Konzept: Register- und Systemverbund (RSV) als Attributs-provider bzw. -Handler insbesondere zur Umsetzung des Once Only-Prinzips in der österreichischen Verwaltung, 18 October 2018.

Federal Data Protection Act (Bundesdatenschutzgesetz).

Fiscal Procedure Code (Codul de Procedură Fiscală) (Romania). https://lege5.ro/Gratuit/g4ztkmrygm/codul-de-procedura-fiscala-din-2015

Funding principles for the authorisation of Grants from the ESF Plus in the Funding period 2021-2027 - Germany (Fördergrundsätze für die Bewilligung von Zuwendungen aus dem ESF Plus in der Förderperiode 2021-2027), (2022).

Gaughran v. the United Kingdom,, CE:ECHR:2020:0213JUD004524515 (European Court of Human Rights, Judgment (First Section) of 13 February 2020).

General Inspectorate for Financial Relations with the European Union (IGRUE), IGRUE-Ispettorato Generale per i Rapporti finanziari con l'Unione Europea. https://www.rgs.mef.gov.it/VERSIONE-I/e_government/amministrazioni_pubbliche/igrue/index.html

Government Decision No 520 of 24 July 2013 on the organisation and functioning of the National Tax Administration Agency (Hotărârea Guvernului Nr. 520 din 24 iulie 2013 privind organizarea şi funcționarea Agenției Naționale de Administrare Fiscală) (Romania).

Guidelines on the conditions of collection and transmission of data in electronic form for the period 2014-2020 (Wytyczne w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020) (Poland).

IAL FVG, IALweb. https://www.ialweb.it/

Istat - Istituto Nazionale di Statistica, Scheda standard di qualità - registro statistico delle imprese attive (ASIA - IMPRESE). Retrieved 2023 from https://www.istat.it/it/archivio/216767

Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294 (Court of Justice of the European Union, Judgment of the Court, 20 May 2003). https://curia.europa.eu/juris/document/document.jsf?text=&docid=48330&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2465139

Joined Cases C-37/20 and C-601/20, Luxembourg Business Registers. ECLI:EU:C:2022:912, Court of Justice of the European Union, Judgment of the Court (Grand Chamber) 22 November 2022., para.45 et seq.

Judgment 17/2013 of 31 January 2012, BOE [Official Gazette] number 49, of 26 February 2013 (Constiutional Court).

Judgment 76/2019 of 22 May 2019, BOE [Official Gazette] number 151, of 25 June 2019 (Constitutional Court).

Judgment 292/2000 of 30 November 2000, BOE [Official Gazette] number 4, of 04 January 2001 (Constitutional Court). https://hj.tribunalconstitucional.es/HJ/en/Resolucion/Show/4276

Labour Market Service Act (Arbeitsmarktservicegesetz) (Austria).

Law 9/2014, of 9 May, General Telecommunications (Ley 9/2014, de 9 de mayo, General de Telecomunicaciones) (Spain).

Law 12/1989, of 9 May, on the Government Statistics Act (Ley 12/1989, de 9 de mayo, de la Función Estadística Pública) (Spain).

Law 19/2013, of 9 December, on transparency, access to public information and good governance, *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*. https://www.boe.es/eli/es/l/2013/12/09/19/con

Law 37/2007 of 16 November 2007 on the reuse of public sector information, *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público*. https://www.boe.es/eli/es/l/2007/11/16/37/con

Law 39/1995, of December 19, on the Organization of the Sociological Research Center (Ley 39/1995, de 19 de diciembre, de Organización del Centro de Investigaciones Sociológicas) (Spain).

Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas) (Spain).

Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations, *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*. https://www.boe.es/eli/es/l/2015/10/01/39/con

Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*.

Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Romania).

Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Romania).

Law No. 571 of December 22, 2003 regarding the Fiscal Code (Romania).

Law on Information Technology, Data Files and Civil Liberties (Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

Law relating to the protection of personal data, amending Loi n°78-17 du 6 janvier 1978 (Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952

Legislative Decree No 82/2005, *DECRETO LEGISLATIVO 7 marzo 2005, n. 82* (Digital Administration Code). https://www.normattiva.it/eli/id/2005/05/16/005G0104/CONSOLIDATED

Legislative Decree No 196 of 30 June 2003 - Personal Data Protection Code, containing provisions for the adaptation of the national system to Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC. (Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679) (Italy). https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig

Legislative Decree No 196 of 30 June 2003, *DECRETO LEGISLATIVO 30 giugno 2003, n. 196* (Privacy Code). https://www.normattiva.it/eli/id/2003/07/29/003G0218/CONSOLIDATED

Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales - LOPDGDD (Organic Law 3/2018 on the Protection of Personal Data and the guarantee of digital rights).

Ministero del Lavoro e delle politiche sociali, Computer System for Compulsory Communications, Sistema informatico per le comunicazioni obbligatorie. https://www.co.lavoro.gov.it/co/welcome.aspx

Ministero dell'Economia e delle Finanze, home page. https://www.mef.gov.it/

Ministero dell'Economia e delle Finanze, La trasmissione dei dati. https://www.rgs.mef.gov.it/VERSIONE-I/attivita_istituzionali/monitoraggio/spesa_per_le_opere_pubbliche/la_trasmissione_dei_dati/

OECD. (2020). *Impact evaluation of labour market policies through the use of linked administrative data*. https://www.oecd.org/els/emp/Impact_evaluation_of_LMP.pdf

Operational programmes within the Framework of the objective "Investment for Growth and Employment" - Austria (Operationelle Programme im Rahmen des Ziels "Investitionen in Wachstum und Beschäftigung"), (2014).

Opinion of the Data Protection Authority on the draft assessment of the Federal Act amending the 1950 Epidemia Act and the COVID-19 Measures Act, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 5 March 2021). https://www.parlament.gv.at/PAKT/BEST/SN/index.shtml

Opinion of the President of the Office on the draft regulation of the Minister of Family, Labour and Social Policy amending the regulation on social welfare homes to the problem of the functioning of the COVID-19 outbreak, 04 September 2020. https://uodo.gov.pl/pl/file/3752

Opinion on Draft Amendment to the 2012 Health Telematics Act, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 17 January 2020). https://www.parlament.gv.at/PAKT/BEST/SN/index.shtml

Opinion on Emergency Ordinance (OUG) 115/2020, which provides for the issuing of digital social vouchers of 180 lei per month for hot meals to people over 75 years of age whose income is at the level of social allowance and to the homeless, with the necessary amounts to be provided from non-reimbursable external funds, 07 April 2021, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro

Opinion on Employee Data Processing in the Context of Telework Activity, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro

Opinion Opinion on Draft Federal Act amending the 1950 Epidemic Act, the Tuberculosis Act and the COVID-19 Measures Act, (Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority), 16 August 2020 2020). https://www.parlament.gv.at/PAKT/BEST/SN/index.shtml

Order CTE/711/2002, of 26 March, laying down the conditions for the provision of the telephone enquiry service on subscriber numbers (Orden CTE/711/2002, de 26 de marzo, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado) (Spain).

Ordinance (2007:907) containing instructions for the Swedish ESF Council (Förordning (2007:907) med instruktion för Rådet för Europeiska socialfonden i Sverige) (Sweden), (2007). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2007907-med-instruktion-for-radet_sfs-2007-907#:~:text=Chefen%20f%C3%B6r%20enheten%20beslutar%20i,besluta%20om%20en%20s%C3%A5dan%20delegering.

Ordinance (2014:1374) on the management of the Fund for European Aid to the Most Deprived (Förordning (2014:1374) om förvaltning av fonden för europeiskt bistånd till dem som har det sämst ställt) (Sweden), (2014). https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20141374-om-forvaltning-av-fonden_sfs-2014-1374

Ordinance (2015:62), Section 9. (Sweden)

Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).

Osservatorio Mercato del Lavoro: PUF 4.0 – GUIDA A MERCURIO Storia, contenuto e specifiche. (2021). Veneto Lavoro Retrieved from https://www.venetolavoro.it/documents/10180/16486105/PUF+Mercurio+-+guida+all%27uso+%28ver+2021-12%29.pdf/b0b25409-6d79-2579-b105-a62e93767a32?t=1640170964620

Peter Puškár v Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy. Request for a preliminary ruling from the Najvyšší súd Slovenskej republiky — Slovakia,, OJ C 402, (Court of Justice of the European Union, Judgment of the Court (Second Chamber) of 27 September 2017 2017).

Proceedings brought by B., Request for a preliminary ruling from Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia),, EU:C:2021:504 (Court of Justice of the European Union, Judgment of the Court (Grand Chamber) of 22 June 2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62019CJ0439&qid=1665649009610

Processing of health data, 18 March 2020, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/?page=Prelucrarea_datelor_privind_starea_de_sanatate&lang=ro

Programmes ESF Plus 2021-2027 Bund - Germany (ESF Plus Programm 2021 - 2027 Bund).

Procedimiento Nº 0049/2020 (2020b). (Of the Spanish Data Protection Agency)

Procedimiento N.º E/06406/2020, (2021a). https://www.aepd.es/es/documento/e-06406-2020.pdf (Of the Spanish Data Protection Agency)

Procedimiento Nº 0029/2021, (2021b). (Of the Spanish Data Protection Agency)

Procedimiento Nº 0032/2021, (2021c). (Of the Spanish Data Protection Agency)

Procedimiento Nº 0075/2020, (2021d). (Of the Spanish Data Protection Agency)

Procedimiento Nº 0078/2020, (2021e). (Of the Spanish Data Protection Agency)

Procedimiento Nº: 0060/2021, (2021f). (Of the Spanish Data Protection Agency)

Regione Marche, Home Page. https://www.regione.marche.it/

Regione Umbria, SiruWEB. https://www.regione.umbria.it/por-fse/siru-fse

Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Regulation (EU) 2021/1057 of the European Parliament and of the Council of 24 June 2021 establishing the European Social Fund Plus (ESF+).

Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy (CPR)

Regulation (EU) No 1303/2013 of the European Parliament and of the Council of 17 December 2013 laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund and repealing Council Regulation (EC) No 1083/2006, OJ L 347, 20. 12. 2013, pp. 320-469. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013R1303

Regulation (EU) No 1304/2013 of the European Parliament and of the Council of 17 December 2013 on the European Social Fund and repealing Council Regulation (EC) No 1081/2006, OJ L 347, 20. 12. 2013, pp. 470-486. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013R1304

Report 31/2020, of 7 April, on the possible transfer to the CIS, by the National Statistics Institute (INE), of the landline and mobile telephones of the population selected in the samples to carry out the functions attributed to the CIS (Informe 31/2020, de 7 de abril relativo a la posible cesión al CIS, por parte del Instituto Nacional de Estadística (INE) de los teléfonos fijos y móviles de la población seleccionada en las muestras para ejecutar las funciones atribuidas al CIS) (Spain).

Report 35/2020 of 27 April, concerning the communication by the CNMC to the CIS of the fixed and mobile telephones of the selected and mobile telephones of the population selected in the nominative samples which are prepared for the CIS by the INE (Informe 35/2020, de 27 de abril, relativo a la comunicación por la CNMC al CIS de los teléfonos fijos y móviles de la población seleccionada en las muestras nominativas que son elaboradas para el CIS por el INE) (Spain).

Republik Österreich Datenschutzbehörde (Austrian Data Protection Authority). (2021). *Information from the data protection authority on the coronavirus (Covid-19)(Information der Datenschutzbehörde zum Coronavirus (Covid-19))*. https://www.dsb.gv.at/download-links/informationen-zum-coronavirus-covid-19-.html

Resolution of 20 March 2013, of the Telecommunications Market Commission, publishing Circular 1/2013, regarding the procedure for the provision of subscriber data for the provision of directory services, telephone enquiries about subscriber numbers and emergencies (Resolución de 20 de marzo de 2013, de la Comisión del Mercado de las Telecomunicaciones, por la que se publica la Circular 1/2013,

relativa al procedimiento de suministro de datos de los abonados para la prestación de servicios de guías, consulta telefónica sobre números de abonado y emergencias) (Spain).

Resolution of 22 December 2021, of the Secretary of State for Social Rights, publishing the Agreement of the Territorial Council of Social Services and the System for Autonomy and Care for Dependency, on the programming of the European Social Fund Plus, in relation to the objective of combating material deprivation (Resolución de 22 de diciembre de 2021, de la Secretaría de Estado de Derechos Sociales, por la que se publica el Acuerdo del Consejo Territorial de Servicios Sociales y del Sistema para la Autonomía y Atención a la Dependencia, sobre la programación del Fondo Social Europeo Plus, en relación con el objetivo de lucha contra la privación material) (Spain).

Review of draft Government Emergency Ordinance no. 19/2020 on the draft Government Decision on the budget and expenditure categories for the population and housing census in Romania in 2021 as well as the establishment of measures on the implementation of certain provisions of Government Emergency Ordinance no. 19/2020, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro

Review of draft Government Emergency Ordinance on granting free days to parents for the supervision of children, in the event of the suspension of courses or the temporary closure of some educational establishments due to the spread of the coronavirus SARS — COV-2. (Gov Emergency Ordinance 147/2020), 24 September 2020, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro

Review of draft Government Emergency Ordinance on taking measures for the proper functioning of the education system and amending and supplementing the National Education Law no. 1/2011, 29 July 2020, (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Romanian NSA, ANSPDCP)). https://www.dataprotection.ro/index.jsp?page=Rapoarte%20anuale&lang=ro

Rotaru v. Romania, CE:ECHR:2000:0504JUD002834195 (European Court of Human Rights, Jugment (Grand Chamber) of 4 May 2000).

Royal Decree 311/2022 of 3 May, which regulates the National Security Scheme, *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*.

Royal Decree 424/2005 of 15 April 2005 approving the Regulation on the conditions for the provision of electronic communications services, universal service and the protection of users (Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios) (Spain).

S. and Marper v. the United Kingdom,, CE:ECHR:2008:1204JUD003056204 (European Court of Human Rights, Judgment (Grand Chamber) of 4 December 2008).

Shimovolos v. Russia,, CE:ECHR:2011:0621JUD003019409 (European Court of Human Rights, Judgment (First Section) of 21 June 2011).

Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF),, OJ C 381 (Court of Justice of the European Union, Judgment of the Court (Third Chamber) of 1 October 2015 2015). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CA0201&qid=1665651259899

Social Insurance Organisation Act (Sozialversicherungs-Organisationsgesetz) (Austria).

Spanish Administrative Unit of the European Social Fund (UAFSE) https://www.mites.gob.es/uafse_2000-2006/uk/bienveni.htm.

'SS' SIA v Valsts ieņēmumu dienests. (Traitement des données personnelles à des fins fiscales) Request for a preliminary ruling from the Administratīvā apgabaltiesa (Regional Administrative Court, Latvia),, EU:C:2021:690 (Court of Justice of the European Union, Opinion of AG Bobek delivered on 2 September 2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CC0175&qid=1665660436180

Statistics Austria, Home Page. https://www.statistik.at/en

Special Directive of the Federal Minister for Work, Social Affairs and Consumers protection on the implementation of projects in the framework of the European Social Fund (ESF) 2014-2020 - Austria (Sonder-Richtlinie des Bundesministers fuer Arbeit, Soziales, und Konsumentenschutz zur Umsetzung von Projekten im Rahmen des Europaeischen Sozialfonds (ESF) 2014-2020), (2019).

Svenska ESF-rådet, Svenska ESF-rådets indikatormodell för Europeiska socialfonden+ 2021–2027, Version 2, 2022 (Swedish ESF Council, Swedish ESF Council Indicator Model for the European Social Fund+ 2021-2027, Version 2, 2022).

Swedish ESF Council regulations and general advice on ESF support under the national social fund programme (Svenska ESF-rådets föreskrifter och allmänna råd om stöd från Europeiska socialfonden inom ramen för det nationella socialfondsprogrammet).

Taylor, M. J., & Whitton, T. (2020). Public Interest, Health Research and Data Protection Law: Establishing a Legitimate Trade-Off between Individual Control and Research Access to Health Data. *Laws*, *9*(1). https://doi.org/10.3390/laws9010006

The Holy Monasteries v. Greece, nos. 13092/87 and 13984/88 (European Court of Human Rights, Judgment (Chamber) of 9 December 1994).

The Italian DPA, 2019, Manuale RPD Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea (Regolamento (UE) 2016/679) (DPO Manual Guidelines for Data Protection Officers in the public and para-public sectors for compliance with the EU General Data Protection Regulation).

Train company (RENFE) and COVID data, E/03689/2020, (2020c). https://www.aepd.es/es/documento/e-03689-2020.pdf

Treaty on European Union (TEU).

Treaty on the Functioning of the EU (TFEU).

TVFS 2016:1 – provisions on ESF 2014-2020 from the Swedish Agency for Economic and Regional Growth, on obligations to share information. .

Unemployment Insurance Act (Arbeitslosenversicherungsgesetz) (Austria).

Veneto Lavoro, Come richiedere Mercurio. https://www.venetolavoro.it/contenuti-del-sito/-/asset_publisher/kB7hwylekZ1z/content/come-richiedere-mercurio

Veneto Lavoro, Sistema Informativo Lavoro Veneto. https://www.venetolavoro.it/silv

Veneto Lavoro, Veneto Lavoro. https://www.venetolavoro.it/chi-siamo

Vooren, M., Haelermans, C., Groot, W., & Maassen van den Brink, H. (2019). The effectiveness of active labour market policies: A meta-analysis. *Journal of Economic Surveys*, *33*(1), 125-149. https://doi.org/https://doi.org/10.1111/joes.12269

Vukota-Bojić v. Switzerland, CE:ECHR:2016:1018JUD006183810 (European Court of Human Rights, Judgment (Third Section) of 18 January 2017).

Vyriausioji tarnybinės etikos komisija, ECLI:EU:C:2022:601 (Court of Justice of the European Union 2022). https://curia.europa.eu/juris/liste.jsf?language=en&jur=C%2CT%2CF&num=C-184/20&parties=&dates=error&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&alldocrec=alldocrec&docdecision=docdecision&docor=docor&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoor=docnoor&docppoag=docppoag&radtypeord=on&newform=newform&docj=docj&docop=docop&docnoj=docnoj&typeord=ALL&domaine=&mots=&resmax=100&Submit=Rechercher

X and Z v Autoriteit Persoonsgegevens. Request for a preliminary ruling from the Rechtbank Midden-Nederland (District Court, Central Netherlands, Netherlands),, EU:C:2021:822 (Court of Justice of the European Union, Opinion of AG Bobek delivered on 6 October 2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CC0245&qid=1665650857775

8.2. Annex II – List of interviews and additional consultations carried out

Austria

- Interview, BFI Salzburg BildungsGmbH (ESF Beneficiary, Austria), 21 November 2022
- Interview, ÖSB Consulting (ESF Beneficiary, Austria), 09 November 2022
- Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022
- Interview, Bundesministerium Bildung, Wissenschaft und Forschung (Data Protection Officer, Austria), 8 November 2022
- Interview, Austrian Data Protection Authority, 17 October 2022.

- Additional consultations, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 30 January 2023, 22 May 2023, and 05 June 2023
- Additional consultation, BFI Salzburg BildungsGmbH (ESF Beneficiary, Austria), 30 January 2023

France

- Interview, Regional Council of Centre-Val de Loire (Beneficiary, France), 20 October 2022
- Interview, La Voix du Client (Evaluator, France), 24 October 2022.
- Interview, Enterprise and Solidarity Pole (managing authority, Normandie, France), 14 November 2022
- Interview, Ministry of Labour, Employment and Inclusion (managing authority, France), 17 October 2022
- Interview, CNIL - Commission nationale de l'informatique et des libertés, 25 October 2022

Germany

- Interview, Bundesministerium für Arbeit und Soziales – BMAS (managing authority, Germany), 18 October 2022.
- Interview, DRK Landesverband Sachsen-Anhalt (Beneficiary, Germancy), 10 November 2022
- Interview, VfBB Speyer (Beneficiary, Germany), 02 November 2022
- Interview, Ministerium für Wirtschaft, Arbeit und Energie, Land Brandenburg (managing authority, Germany), 20 October 2022
- Interview, Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen (managing authority, Germany), 02 November 2022
- Interview, Institute for social-pedagogical research Mainz (Evaluator, Germany), 6 October 2022
- Additional consultation, Bundesministerium für Arbeit und Soziales – BMAS (managing authority, Germany), 21 February 2023
- Additional Consultation, Ministerium für Wirtschaft, Arbeit und Energie, Land Brandenburg (managing authority, Germany), 27 February 2023

Ireland

- Interview, Department of Social Protection 1 (Intermediary body for Aid to the Most Deprived, Ireland), 14 November 2022.
- Interview, Department of Social Protection 2 (Intermediary body, Back to Work Enterprise Allowance scheme), 21 November 2022.
- Interview, Department of Social Protection 3 (Intermediary body, JobPlus Youth scheme), 21 November 2022.
- Interview, HEA- Higher Education Authority (Intermediary body, Ireland), 16 November 2022.
- Interview, WAP - Waterford Area Partnership (Beneficiary, Ireland), 15 November 2022.
- Interview, Pobal (Beneficiary SICAP, Ireland), 10 November 2022
- Interview, PEIL (managing authority, Ireland), 12 October 2022
- Additional consultation, Department of Social Protection, 14 June 2023

Italy

- Interview, Innovazione Apprendimento Lavoro Friuli Venezia Giulia (ESF Beneficiary, Italy), 26 October 2022
- Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 03 November 2022
- Interview, Marche Region (ESF managing authority, Italy), 21 October 2022
- Interview, Ministry of Economy and Finance – IGRUE (Administrative Data Holder, Italy), 26 October 2022
- Interview, The Italian Data Protection Authority, 03 November 2022
- Additional consultations, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 31 May 2023, and 06 June 2023

Poland

- Interview, OpenField (Evaluator, Poland), 20 October 2022
- Interview, Employment Office of the Capital City of Warsaw (Administrative data holder, Poland), 27 October 2022
- Interview, Ministry of Funds and Regional Development (managing authority, Poland), 31 November 2022.
- Interview, Office for Protection of Personal Data (Poland), 14 November 2022

- Interview, Main Statistical Office (Poland), 31 November 2022
- Additional consultation, Ministry of Funds and Regional Development (managing authority, Poland), 02 February 2023

Romania

- Interview, University of Bucharest (Beneficiary, Romania), 24 October 2022
- Interview, National Unemployment Agency (managing authority, Romania)
- Interview, UEFISCDI (managing authority, Romania),
- Interview, The Romanian National Statistical Institute, 28 October 2022
- Interview, National Supervisory Authority for Personal Data Processing (Romania), 14 December 2022
- Additional consultation, National Unemployment Agency (managing authority, Romania), 30 January 2023

Spain

- Interview, Red2Red (evaluator, Spain), 19 October 2022
- Interview, UAFSE - Spanish Administrative Unit of the European Social Fund (managing authority, Spain), 15 November 2022
- Interview, Mancomunidad Intermunicipal Alto Palancia (Beneficiary, Spain), 04 November 2022
- Interview, UCM - General Foundation of Universidad Complutense de Madrid (Beneficiary, Spain), 08 November 2022
- Interview, Spanish Data Protection Agency, 18 October 2022
- Interview, Statistical Institute (Region of Valencia, Spain), 28 October 2022
- Interview, Eustat (Statistical Institute, Basque Country, Spain), 16 November 2022
- Additional consultations, Red2Red (evaluator, Spain), 16 February 2023, and 30 May 2023
- Additional consultation, UAFSE - Spanish Administrative Unit of the European Social Fund (managing authority, Spain), 25 May 2023
- Additional consultation, UCM - General Foundation of Universidad Complutense de Madrid (Beneficiary, Spain), 09 February 2023

Sweden

- Interview, Arbetsförmedlingen (Beneficiary and administrative data holder, Sweden), 13 October 2022
- Interview, Trygghetsfonden TSL (Beneficiary, Sweden), 14 October 2022
- Interview, an anonyme consultancy (Evaluator, Sweden), 17 October 2022
- Interview, Statistics Sweden (SCB), 10 October 2022
- Interview, The Swedish ESF Council (managing authority), 17 October 2022

8.3. Annex III – Interview country summaries

8.3.1. Austria

Types of data collected and used

ESF participant data

One beneficiary that is an educational institute collects the following information from participants of its projects[484]: name, address, phone number, e-mail address, date of birth, social security number, nationality, mother tongue, highest level of education, employment status, education at project entry, and special characteristics such as foreign origin, member of minority, disabilities, or other disadvantages.

Another beneficiary that implements labour related ESF projects collects similar data from its participants, including the following: name, address, date of birth, gender, entry date, exit date, employment status, education, and special characteristics such as foreign origin, member of minority, disabilities, and social disadvantages[485].

The information on the proof of participation (name, date of birth, gender, contact details as well as the date of entry and exit) and on the proof of belonging to the eligible target group are absolutely necessary for compliance with the audit trail. Participants in ESF-funded projects are obliged to provide this minimum information, otherwise the costs incurred would no longer be eligible for funding and would not be reimbursed[486]. When beneficiaries collect data from participants, they are informed about the use of the data and sign to give their consent. The data are then transferred to the managing authority[487].

Administrative data

The BMAW managing authority use or plan to use existing administrative data for both monitoring and evaluation purposes. For monitoring purposes, this includes employment status collected from the social security register to feed the EECR05 ESF indicator on participants in employment, including self-employment, six months after leaving. For evaluation purposes, data will include AMS-DWH (Public Employment Service Data Warehouse), employment status and income from Main Association of Social Insurances School statistics (BilDok, BibEr)[488].

Storing data

Three interviewees mentioned that they store collected data in the ESF ZWIMOS database, which is managed by the managing authority. It includes both monitoring and evaluation

[484] Interview, BFI Salzburg BildungsGmbH (ESF Beneficiary, Austria), 21 November 2022.

[485] Interview, ÖSB Consulting (ESF Beneficiary, Austria), 09 November 2022.

[486] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[487] Interview, ÖSB Consulting (ESF Beneficiary, Austria), 09 November 2022.

[488] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

relevant data, and the information about individual ESF participants. The managing authority is obliged by law to store data in this database[489].

Transferring data[490]

Transferring participants' personal data

In Austria, the participants of ESF-funded projects have explicitly consented to the use of their data and the transfer of data, including special categories of personal data to the Federal Ministry of Labour for the purpose of evaluation. The data sheet must be signed by each participant. Participant data are transferred via the ESF ZWIMOS database which the managing authority has access to. If evaluators need to access these data, they can request it from this database too. However, research institutes receive data only in pseudo-anonymised form[491].

Transferring administrative data

The process of transferring administrative data for ESF evaluation purposes is managed centrally by the managing authority BMAW. For evaluations and impact analyses, evaluators must request data from the ZWIMOS database through BMAW and link and compare it with data from the AMS-DWH database. If this procedure does not result in a sufficient person match, then an additional attempt should be made to supply the data with additional steps according to certain procedures of BMAW. Pseudo-anonymisation is done via an external service provider[492].

Using and linking data

As described above, different databases are linked to compare data and match individuals' data for comparison. However, most data are collected directly from participants as the indicators vary too much between different datasets. These differences make the process very time consuming[493].

Challenges

In the previous programming period, the Austrian DPA did not agree to the use of social security numbers for evaluation purposes. However, this has changes for the ESF+ period, which makes it easier to access and compare data. Still, one big challenge is that it is extremely time-consuming to make the data usable for evaluation purposes while complying

[489] (1) Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022. (2) Interview, BFI Salzburg BildungsGmbH (ESF Beneficiary, Austria), 21 November 2022. (3) Interview, ÖSB Consulting (ESF Beneficiary, Austria), 09 November 2022.

[490] The expression 'data transfer' in the context of this study refers to the act of transmission of data and not transfer of data outside EU/EEA legal space. As this interview country summaries are based on interview questionnaires that use the term 'data transfer' the terminology has not been changed.

[491] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[492] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[493] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

with data protection regulations. It requires a data extract from the register, which must be interlinked with the data of the ESF database. Moreover, the data must be pseudo-indexed and only this data set is available for evaluation purposes. This process requires the involvement of several institutions, and all processes must run centrally via the managing authority. Due to the high financial and personnel costs, such data provision can only be justified for individual evaluation questions for which access to data can be facilitated by the managing authority. The second problem is that the statistics are often available with a long-time lag, sometimes only a year or more. If a follow-up period of several years is included, it becomes difficult to provide the evaluation results at a time when they can still be used meaningfully in the programme implementation cycle[494].

Another challenge, regarding the collection of data from participants was mentioned by an ESF beneficiary. After registration of participants for qualification check, they cannot get any information about who has or has not qualified to participate in the ESF project. Thus, if they do not get this information directly from participants, there is no way of receiving this information[495].

Potential solutions/good practices

Linking personal data through a unique number: One of the basic prerequisites for the analysis of the effect of participation on further employment is the identification of the persons supported, while maintaining data protection. In the Austrian register data, persons are assigned a unique anonymous number (PENR). For example, the labour market and employment career database of L&R Social Research contains a unique anonymous number with the PENR for all persons insured in Austria since 1997. Due to the indirect personal reference, no conclusions can be drawn about individual persons. The ESF funding data, on the other hand, does not contain any unambiguously assignable personal numbers. They therefore had to be identified through a multi-stage process using the personal details recorded in the ESF database (first name, surname, date of birth). This pseudonymisation process was carried out by experts from the Federal Ministry of Labour and the Public Employment Service[496].

Guidance/advice

The Austrian DPA has not been contacted or issued any guidance related to ESF. However, several interviewees mentioned that they have had internal advice and training. For example, GDPR training is mandatory for all employees of ÖSB Consulting. Moreover, the beneficiary BFI Salzburg BildungsGmbH has a DPO that advises and provided the data collection and privacy management templates. BMAW finds data protection guidance by internal lawyers necessary. However, BMAW mentioned in the interview that they need more guidance; for example, regarding the question to what extent the ESF regulation provides a sufficient legal basis for collecting the indicators or whether the participants' consent is required and especially for special categories of data such as on disabilities. Clarifications on this matter are needed as soon as possible because it determines the information provided to ESF participants on the consent form[497].

[494] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[495] Interview, BFI Salzburg BildungsGmbH (ESF Beneficiary, Austria), 21 November 2022

[496] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

[497] Interview, BMAW - Bundesministerium für Arbeit und Wirtschaft (ESF managing authority, Austria), 10 October 2022.

8.3.2. France

Types of data collected and used

ESF participant data

The ESF beneficiary Regional Council of Centre-Val de Loire, who provides trainings, explained the following data collection steps and which information they collect[498].

- Before the training: name, surname, date and place of birth, address, phone number, whether a parent is from outside of France, type of training, household situation, handicap, occupation status (work/education), and which organisation that implemented the training.

- After the training: name, surname, whether they completed the training and if not for which reason (job, other training, started a company, health reasons, etc.), and whether they succeeded. The questionnaire also includes questions on the situation maximum four weeks after the training (working, training, looking for a job, inactive, company), if the person is working, the type of job (permanent, temporary, seasonal, etc.), and whether it is linked to the training. Participants must also mention whether they have received an offer for a job, training or traineeship.

- In addition, trainees who are eligible for remuneration must fill in another document where they have to indicate information on their civil status, family situation, social protection regime, level of education, previous working or training activities, handicap, and work status.

Moreover, other interviewees stated that information such as name and employment status is collected from participants[499].

Administrative data

While the managing authority at the Ministry of Labour stated that they do not use administrative data[500], the evaluator La Voix du Client did, via the Ma Démarche FSE database, but without specifying what type of data[501]. The beneficiary Regional Council of Centre-Val de Loire has requested verification data from the national institution Pole Emploi to check whether participants are registered as jobseekers or not but have not been able to access such data[502].

[498] Interview, Regional Council of Centre-Val de Loire (Beneficiary, France), 20 October 2022.

[499] (1) Interview, La Voix du Client (Evaluator, France), 24 October 2022. (2) Interview, Enterprise and Solidarity Pole (managing authority, Normandie, France), 14 November 2022.

[500] Interview, Ministry of Labour, Employment and Inclusion (managing authority, France), 17 October 2022.

[501] Interview, La Voix du Client (Evaluator, France), 24 October 2022.

[502] Interview, Regional Council of Centre-Val de Loire (Beneficiary, France), 20 October 2022.

Storing data

The evaluator La Voix du Client explained that information about participants is stored centrally in the Ma Démarche FSE database. In addition, each region has different systems, and some have databases similar to the national one[503]. The Centre-Val de Loire region has such a database, where beneficiaries store data about participants[504].

Transferring data

Transferring participants' personal data

Participant data is transferred through central databases at a regional level and to the national Ma Démarche FSE database. Through this database, both managing authorities and evaluators have access to the participant data. For evaluations, the evaluator La Voix du Client has access to this data from both the national and the regional databases upon agreement with the managing authority[505]. No direct distinction is made between types of information[506].

Transferring administrative data

No concrete information was given on transfer of administrative data.

Using and linking data

No concrete information was given on linking data.

Challenges

As mentioned above, beneficiaries may not be able to verify participants' employment status through Pole Emploi due to GDPR concerns. Moreover, challenges for beneficiaries include unclarities regarding which documents that are possible to request to prove different types of data (such as a person's age) and what is considered as a safe transfer method[507].

The Normandie managing authority mentioned that while there are no specific data protection challenges to talk about, the practical procedure can be difficult. However, the new system with the Ma Démarche FSE database might solve some of those issues[508].

[503] Interview, La Voix du Client (Evaluator, France), 24 October 2022.

[504] Interview, Regional Council of Centre-Val de Loire (Beneficiary, France), 20 October 2022.

[505] Interview, La Voix du Client (Evaluator, France), 24 October 2022.

[506] (1) Interview, La Voix du Client (Evaluator, France), 24 October 2022. (2) Interview, Enterprise and Solidarity Pole (managing authority, Normandie, France), 14 November 2022.

[507] Interview, Regional Council of Centre-Val de Loire (Beneficiary, France), 20 October 2022.

[508] Interview, Enterprise and Solidarity Pole (managing authority, Normandie, France), 14 November 2022.

Potential solutions/good practices

No concrete solutions were mentioned.

Guidance/advice

All interviewees mentioned that they have received data protection guidance in one form or another. For example, via in-house specialists[509] or contracted private actors[510]. The Ministry of Labour does not have any problem to follow data protection rules and does not need any additional advice. However, they follow guidelines and take part in evaluation meetings with DG EMPL[511]. The evaluator La Voix du Client received concrete guidelines from the managing authority on how to access administrative data and how to use it, which is helpful. Also, to stop using household information in their evaluations[512].

The French Data Protection Authority (CNIL) stated in the interview[513] that they have been asked on several occasions for its opinion on draft texts providing for the introduction of teleservices enabling project promoters to contact the ESF and to send it the information necessary for this purpose. This information may include personal data. However, in the projects on which the CNIL worked, the data was collected directly from the persons concerned (and not from public bodies).

The CNIL did not interact with authorities that reuse personal administrative data collected for the purpose of monitoring or evaluating ESF programmes. Nor has it undertaken any data protection audits on data protection of ESF monitoring and evaluation. However, CNIL provided guidance on multiple occasions and have recalled that only data relevant to the purpose of the processing operation could be transmitted to the ESF. CNIL made recommendations not to process certain categories of data which did not seem useful for the projects referred to it. It also questioned the precision, objectivity and appropriateness of certain terms used (e.g., the statistical definition of persons of foreign origin), as well as the legality of collecting certain data (membership of 'ethnic minorities') under French law. In this regard, it recommended that only objectively definable categories of data be used (e.g., commune of birth and nationality of parents).

The CNIL was asked to comment on the draft processing operations 'Ma démarche FSE' (opinion available online) and 'Synergie' (opinion available online). The types of data include immigration records' data, employment/jobseeker registers and social service registers.

More precisely, the points of vigilance raised by the CNIL include the respect of intellectual property rights, the concealment of certain information, the pseudonymisation or anonymisation of data, the obligation to update data, the obligation to notify and the professional secrecy where applicable.

For the time being, the CNIL's work has focused on the dissemination of public data, which concerns the data of public actors and private persons entrusted with a public service mission. (Work on the framework for the reuse of data also held by private actors is underway). Regarding the exchange of data between administrations, examples of processing concern immigration records data, police or courts records, and health records.

[509] Interview, Enterprise and Solidarity Pole (managing authority, Normandie, France), 14 November 2022.

[510] Interview, Regional Council of Centre-Val de Loire (Beneficiary, France), 20 October 2022.

[511] Interview, Ministry of Labour, Employment and Inclusion (managing authority, France), 17 October 2022.

[512] Interview, La Voix du Client (Evaluator, France), 24 October 2022.

[513] Interview, CNIL - Commission nationale de l'informatique et des libertés, 25 October 2022.

Moreover, CNIL has published a 'Practical guide to publishing and re-using data', a Practical guide to authorised third parties and a Draft technical recommendation on the use of application programming interfaces (APIs) for the secure sharing of personal data submitted for public consultation.

8.3.3. Germany

Types of data collected and used

ESF participant data

Data collected from participants mentioned during the interviews include name, address, e-mail address, phone number, and employment status including six months after leaving[514]. However, for some beneficiaries, the data collected mostly depend on the project and specific funding requirements[515].

Administrative data

The only interviewee that explicitly mentioned that they use administrative data was the Brandenburg Ministry of Labour, for monitoring and not evaluations. Data can include percentage of disabled people and migration background and comes from different sources[516]. The managing authority and the federal ministry of labour mentioned that administrative data has been used only once. At that occasion, it was used to gather information on the indicator "participants in employment, including self-employment, six months after leaving". However, the managing authority did not have lawful access to this data themselves. It was an external evaluator that managed to access this information[517].

Storing data

Data storage does not seem to be harmonised. Data on participants can be stored internally by beneficiaries, at regional servers, and or by regional managing authorities[518].

[514] (1) Interview, Bundesministerium für Arbeit und Soziales – BMAS (managing authority, Germany), 18 October 2022. (2) Interview, DRK Landesverband Sachsen-Anhalt (Beneficiary, Germancy), 10 November 2022.

[515] Interview, VfBB Speyer (Beneficiary, Germany), 02 November 2022.

[516] Interview, Wirtschaftsministerium arbeit und energie Bradbeburg (managing authority, Germany), 20 October 2022.

[517] Interview, Bundesministerium für Arbeit und Soziales – BMAS (managing authority, Germany), 18 October 2022.

[518] (1) Interview, VfBB Speyer (Beneficiary, Germany), 02 November 2022. (2) Interview, Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen (managing authority, Germany), 02 November 2022.

Transferring data

Transferring participants' personal data

Three interviewees mentioned that participant data is transferred to the relevant managing authority[519]. The North Rhine-Westphalia managing authority mentioned that all beneficiaries collect personal data regarding participants before and after each project. This data is sent anonymised to the North Rhine-Westphalia managing authority. If participants have given their consent, these data are shared with evaluators and the ministry centrally.

Transferring administrative data

The federal managing authority BMAS stated that they cannot request administrative data. Only research institutes can do so. However, the ministry was involved to help the researchers in the application process. The process took about a year and the research institute had to pay for the procedure. The managing authority understands that the procedure differs depending on the government level of the data, and which legal provisions that apply to the specific dataset[520].

Using and linking data

N/A

Challenges

Both managing authorities that were interviewed had similar thoughts about the challenges to access administrative data. These can be summarised as follows[521]:

- Decentralised data processing and storage: administrative data are stored at three levels: federal, regional, and local levels. There are only two central administrative datasets, which are held by the Employment Agency and the Central register for foreigners. Also, many datasets are stored only within individual institutions such as schools. The ESF/ESF+ managing authorities are not allowed to access these due to data protection reasons. Only research institutes and selected authorities may do so.

- Unavailability: some types of data such as certain special categories of personal data including disabilities and regarding minorities are not collected in Germany.

- Data protection rules and a lack of common understanding of the legal context: There might be different rules that apply to different levels or horizontally.

[519] (1) Interview, DRK Landesverband Sachsen-Anhalt (Beneficiary, Germancy), 10 November 2022. (2) Interview, VfBB Speyer (Beneficiary, Germany), 02 November 2022. (3) Interview, Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen (managing authority, Germany), 02 November 2022.

[520] Interview, Bundesministerium für Arbeit und Soziales – BMAS (managing authority, Germany), 18 October 2022.

[521] (1) Interview, Bundesministerium für Arbeit und Soziales – BMAS (managing authority, Germany), 18 October 2022. (2) Interview, Wirtschaftsministerium arbeit und energie Bradbeburg (managing authority, Germany), 20 October 2022.

- Different datasets may not be interoperable.
- There might be no prior consent to transfer data from participants or use it for certain purposes.

Regarding challenges related to personal data of ESF participants, one beneficiary mentioned that, as a small organisation, it is challenging to keep track of legal obligations and changes to data storage requirements[522]. Moreover, the North Rhine-Westphalia managing authority had to remove some questions from questionnaires that are being sent to participants because they did not have any legal basis to collect this information. Collecting this information would have required explicit consent from the participants, which would come with a bureaucratic burden. As a result, they could not report all required data to the ministry[523].

Potential solutions/good practices

It would be helpful if German data protection law was not more restrictive than required by EU law and harmonised between levels of government[524].

An interviewee from the federal managing authority mentioned the recommended method of 'informed estimates' (fundierte Schaetzung) to estimate data of participants as an alternative solution to receive otherwise missing data, without participants' consent, has been denied by national authorities in Germany. It concerns special categories of personal data, such as regarding ethnic minorities and disabilities.[525].

Guidance/advice

Most of the interviewees mentioned that they use internal DPOs to guide the organisations' data protection issues. For example, the North Rhine-Westphalia managing authority had discussions with its DPO, held workshops, and discussed legal solutions for the 2021-2027 funding period, and whether it should make use of another legal basis that does not require explicit consent[526]. Moreover, one beneficiary interviewed stated that despite forms and instructions from the managing authority, extensive training is needed to guide them through the different data protection issues[527].

[522] Interview, VfBB Speyer (Beneficiary, Germany), 02 November 2022.

[523] Interview, Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen (managing authority, Germany), 02 November 2022.

[524] Interview, Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen (managing authority, Germany), 02 November 2022.

[525] Interview, Bundesministerium für Arbeit und Soziales – BMAS (managing authority, Germany), 18 October 2022.

[526] Interview, Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen (managing authority, Germany), 02 November 2022.

[527] Interview, DRK Landesverband Sachsen-Anhalt (Beneficiary, Germancy), 10 November 2022.

8.3.4. Ireland

Types of data collected, shared, and or used

ESF participant data

The beneficiaries and intermediary bodies interviewed gave examples of personal information connected to ESF monitoring and evaluation indicators, including sensitive information, financial, and non-financial data. The types of data depend on the programmes and projects involved but may include, depending on the actor and purpose,: name, date of birth, address, e-mail address, phone number, ethnicity, household information, gender, commencement date, completion data, employment status (before and after the projects), education and training history, qualifications gained, national background, disabilities and other disadvantages, minority status, homelessness, residency, and type of area[528].

Administrative data

The managing authority, PEIL, mentioned several data types and databases that are used; However, with restricted access and use for a few institutions depending on the purpose, and not used by themselves. These include[529]

- Data on social protection payments from the Department of Social Protection.
- Employment Registers.
- Pension registers.
- According to the Irish managing authority, data sharing agreements are rare and lengthy processes to conclude in Ireland. Only one example exists in Ireland relevant for the ESF, the Jobseekers Longitudinal Dataset (JLD), which draws together payment and administrative data from the Department of Social Protection and data from SOLAS and the Revenue Commissioners. It contains information on a claimant's sex, age, marital status, nationality, educational attainment, previous occupation, employment and unemployment histories (duration and number of episodes), unemployment training history (type, duration and number of episodes), benefit type, spousal earnings (to qualify for an adult dependent allowance), number of child dependents, family payment type (i.e. adult and child dependent allowances, adult only, etc.) and geographic location. Through the development of the JLD, administrative data events are linked to episodes of welfare or work, thus enabling the better ex ante and ex post analysis of jobseekers.
- A database called PLSS which records further education details (highest education obtained and highest education outcomes) that is run by SOLAS.

[528] (1) Interview, Department of Social Protection 1 (Intermediary body for Aid to the Most Deprived, Ireland), 14 November 2022. (2) Interview, Department of Social Protection 2 (Intermediary body, Back to Work Enterprise Allowance scheme), 21 November 2022. (3) Interview, Department of Social Protection 3 (Intermediary body, JobPlus Youth scheme), 21 November 2022. (4) Interview, HEA- Higher Education Authority (Intermediary body, Ireland), 16 November 2022. (5) Interview, WAP - Waterford Area Partnership (Beneficiary, Ireland), 15 November 2022. (6) Interview, Pobal (Beneficiary SICAP, Ireland), 10 November 2022.

[529] Interview, PEIL (managing authority, Ireland), 12 October 2022.

- A few databases run by the Higher Education Authority into which universities report. One of these is called the Student Records System (SRS). Universities record data of course entry, labour market status, and other things related to higher education and outcomes, if students gain qualifications, if they are still in education or training, etc.

One interviewee from the Department of Social Protection explained that they only use administrative data from their own department. For evaluation purposes, the department has access to anonymised data from their own department, including data on birth, employment status, education, social service consumption, tax, criminal records, etc. Also, on health, but only if individuals get support from the department due to disability or illness. If they were to access data on employment from other ministries such as on employment, they would get general statistics on employment[530].

One beneficiary stated that it can access national registration numbers (PPS number) from the Department of Social Protection. Other data are collected directly from participants or received in the form of public statistics from the Central Statistics Office such as on deprivation status per district and electoral area, which is useful to know in which are support should be concentrated to[531].

Storing data

ESF participant data

Different databases are in place to store and transfer data about ESF participants:

- IRIS, a central CRM database (Microsoft dynamics) that is a participant database for the Social Inclusion Community Activation Programme (SICAP). The database is managed by Pobal. Beneficiaries can only see their own data, and the intermediary bodies and the managing authority can only see anonymised data[532].

- Participants' data is transferred to the managing authority through the e-Cohesion system. The system in owned by the Department of Further and Higher Education, Research, Innovation and Science (DFHERIS). The data is assessed to ensure it can be included in the claim but anonymise/pseudonymisation is not required as it is uploaded to the secure e-Cohesion system[533].

- The Department of Social Protection has a system called BOMi. Participant form responses are electronically uploaded to the Department's BOMi system as a restricted viewing document due to the sensitive nature of some of the data provided e.g., questions on social inclusion, education status. Access to the data would require a Data Protection Impact Assessment and if approved would require a Data Sharing Agreement[534].

[530] Interview, Department of Social Protection 1 (Intermediary body for Aid to the Most Deprived, Ireland), 14 November 2022.

[531] Interview, WAP - Waterford Area Partnership (Beneficiary, Ireland), 15 November 2022.

[532] (1) Interview, WAP - Waterford Area Partnership (Beneficiary, Ireland), 15 November 2022. (2) Interview, Pobal (Beneficiary SICAP, Ireland), 10 November 2022.

[533] Interview, Department of Social Protection 3 (Intermediary body, JobPlus Youth scheme), 21 November 2022.

[534] Interview, Department of Social Protection 2 (Intermediary body, Back to Work Enterprise Allowance scheme), 21 November 2022.

Administrative data

The managing authority mentioned a number of administrative databases that store data that are relevant for ESF monitoring and evaluation[535].

- A database called PLSS which records further education details (highest education obtained and highest education outcomes) that is run by SOLAS.
- The Department of Social Protection administer all databases on social protection payments. The department uses its own administrative databases to supplement the indicators.
- A few databases run by the Higher Education Authority into which universities report. One of these is called the Student Records System (SRS).

Collection of participants' data, consent, and data sharing practices

The different actors interviewed have different data processing practices in place.

The two beneficiaries interviewed reported that they collect data directly from participants and that they must sign a consent form[536]. The beneficiary WAP explained that they receive contact details and national registration numbers from other governmental bodies to identify and collect data from participants. WAP collects and reports enter and exit data such as on employment and education of participants and follow up six months thereafter[537].

One interviewee from the Department of Social Protection explained that data are collected to understand why individuals seek assistance and to report to the European Commission via the managing authority. As the department is an intermediary body, it requests data from participants via the beneficiaries and receives them anonymised[538].

Another interviewee of another unit at the Department of Social Protection stated that the department via beneficiaries collects participants' personal data via surveys before and after projects. Thereafter, the data are provided to the managing authority and an audit authority (DFHERIS) via a secure eCohesion system that does not require anonymisation[539].

Both the Department of Social Protection and the HEA share data about participants to auditors. The interviewee from the intermediary body HEA explained that it receives personal data about participants from beneficiaries (universities) but only regarding enrolled students who have started a course that is involved in the ESF project. The HEA can in theory identify the persons but does not do so. The data are sent to external auditors via safe and password-locked files to check whether the beneficiaries' funding applications are eligible for funding. For this auditing purpose, data are not shared with anyone else[540].

[535] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[536] (1) Interview, WAP - Waterford Area Partnership (Beneficiary, Ireland), 15 November 2022. (2) Interview, Pobal (Beneficiary SICAP, Ireland), 10 November 2022.

[537] Interview, WAP - Waterford Area Partnership (Beneficiary, Ireland), 15 November 2022.

[538] Interview, Department of Social Protection 1 (Intermediary body for Aid to the Most Deprived, Ireland), 14 November 2022.

[539] Interview, Department of Social Protection 2 (Intermediary body, Back to Work Enterprise Allowance scheme), 21 November 2022.

[540] Interview, HEA- Higher Education Authority (Intermediary body, Ireland), 16 November 2022.

The managing authority explained in detail the infrastructure for collecting and sharing data on participants. It explained that the system relies on data sharing agreements that it put in place. These agreements are put in place with the intermediary bodies and beneficiaries for them to collect and transfer data on ESF indicators to the managing authority. Without such an agreement, no data can be transmitted. Most data collection relies on explicit consent from participants. The managing authority does not have its own database. Data according to the ESF indicators are uploaded to the e-Cohesion system. The managing authority does not have direct access to this system and must rely on having the data strictly related to the indicators transferred to them in an aggregated form. According to the managing authority, most data in use for both monitoring and evaluation are data collected directly from participants because it is very hard to access administrative data. The only counterfactual assessments made are done by authorities such as the Department of Social Protection that can rely on their own internal datasets[541].

Use of administrative data and sharing practices for ESF purposes

Administrative data are hard to get hold of in Ireland according to the managing authority. Access to data is easier to gain within government departments than between departments. Most evaluations use data from direct collection of data from participants through surveys, etc.[542].

The Data Sharing and Governance Act 2019 (DSGA) regulates how and when public bodies can share personal data with other public bodies when providing public services. It also establishes the Data Governance Board to promote and advise on compliance with the DSGA. The main obligation is that public bodies must follow the data sharing requirements set out in Part 3 of the DSGA. In summary, this involves identifying a specific provision of law requiring or permitting the data sharing to take place. If no specific provision of law exists, public bodies must take additional steps to comply with the DSGA. These steps include putting in place a data sharing agreement in accordance with Part 4 of the DSGA and submitting this to the Data Governance Board for public consultation. The requirements of the DSGA are in addition to, and not instead of, the requirements under data protection legislation[543].

Intermediary bodies such as the Department of Social Protection, the HEA, and SOLAS can use their own records and complement with surveys for monitoring and evaluating the ESF. For example, SICAP, the Social Inclusion and Community Activation Programme, has used their access to administrative records to do evaluations such as counterfactual impact evaluations. SICAP tried to get access to data from the Live Register (the unemployment register) from the Department of Social Protection for an evaluation. However, they were not able to put an agreement in place in time to have the data shared. What SICAP used instead was the data they collected directly from participants in a survey six months after they completed the programme to ask them about their labour market status. The survey results were used instead for their counterfactual evaluation because they could not get access to data from the Department of Social Protection[544].

Moreover, the Department of Social Protection made a counterfactual evaluation on the Jobs Plus Scheme, which they run themselves. Since it is the same ministry that runs the Live Register, they were able to internally use that data for a counterfactual evaluation. They could track quite clearly the participants' progress up to two years after completion of the

[541] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[542] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[543] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[544] Interview, PEIL (managing authority, Ireland), 12 October 2022.

programme. However, they do not share that data with the managing authority, just the methodology and outcomes in a report[545].

According to the managing authority, it is very hard to get data sharing agreements in place to share information between ministries, for example, on employment status of individuals. The only counterfactual assessment made has been done based on internal data held or direct collection of data from participants. The Government Data Sharing Act was put in place to make it easier to share data between government departments. Parts of it got enforced and other parts were deferred. The parts that were deferred were those that would facilitate data sharing such as for evaluating ESF programmes[546].

The difficulties to share data between governmental departments and the difficulties to conclude data sharing agreements are confirmed in interviews with different units within the Department of Social Protection[547].

However, there are some exceptions, for example, a data sharing agreement between the SOLAS and the Department of Social Protection. Together, these bodies host the JLD. The JLD enables the Department of Social Protection's Statistics and Business Intelligence Unit to track jobseeker journeys including episodes of employment and unemployment together with services received over a prolonged period. This, in turn, facilitates the analysis of the effectiveness of individual services in improving employment outcomes. The development of the JLD was complemented by the formation of a Labour Market Council (LMC) composed of external experts and stakeholders and the development, under its guidance, of an evidence-based approach to the development and operation of the public employment service (PES)[548].

The JLD is an administrative dataset that tracks social welfare claims, activation and training, and employment histories over time, covering people with jobseeker or one parent family claims since 2004. It draws together payment and administrative data from the Department of Social Protection and data from SOLAS and the Revenue Commissioners. It has its origins in efforts to make best use of the sizeable volume of data collected or generated by the Department and to structure the recording of episodes of unemployment and training in a meaningful way[549].

The JLD has been used for a variety of analytical tasks and published evaluations. The JLD is a very rich source of data and is being made available to researchers and academics for the purpose of undertaking research into the labour market and the interplay between the labour market and the State's welfare, employment and further education and training services[550].

[545] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[546] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[547] (1) Interview, Department of Social Protection 1 (Intermediary body for Aid to the Most Deprived, Ireland), 14 November 2022. (2) Interview, Department of Social Protection 2 (Intermediary body, Back to Work Enterprise Allowance scheme), 21 November 2022. (3) Interview, Department of Social Protection 3 (Intermediary body, JobPlus Youth scheme), 21 November 2022.

[548] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[549] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[550] Interview, PEIL (managing authority, Ireland), 12 October 2022.

Linking data

As described above, the intermediary bodies frequently link data from their own registers, participant data and data from monitoring and evaluation surveys. For example, to conduct counterfactual analyses to evaluate the ESF.

Challenges

According to one interviewee from the Department of Social Protection, there are no data protection issues, at least not regarding sharing or gaining access to anonymised data, and there are no differences between the data types[551]. However, an interviewee from another unit within the department stated that data sharing agreements and the difficulties regarding sharing data are challenges[552].

Apart from the challenges regarding data sharing agreements, the managing authority described there being in general a culture of uncertainty when it comes to data protection rules in Ireland. People are simply afraid of making mistakes because it is hard to interpret the laws[553].

One challenge for the HEA concerns them not being allowed to collect special categories of personal data that is required for ESF reporting. Also, it may be hard to access other types of data. Currently, the HEA is exploring the possibility to gain access to Personal Public Service (PPS) numbers of potential participants. The HEA has requested these from the Department of Social Protection, but the process is very time consuming[554].

Moreover, it may be difficult to explain to participants that their data need to be saved for a very long time, and it is hard to know for exactly how long beforehand. The ESF reporting requirements require the HEA to retain data for about seven years, and then extensions to these requirements may occur for another five years. With such uncertainty, it is hard to be clear towards the data subjects. It is difficult to justify storing their data for 13 years. The HEA has consulted the managing authority about this issue[555].

Another challenge that the HEA raised concerns indicators. The contracts that the HEA concludes with beneficiaries include which data connected to ESF indicators they must collect from participants. The problem is that these indicators are defined and communicated by the European Commission too late to include them in the contracts with beneficiaries. Thus, if some indicators are still unknown, they cannot include these in the contracts, and the data will not be collected. Therefore, the HEA has requested clearer monitoring indicators early in the process[556].

Pobal mentioned challenges related to indicators too, especially regarding special categories of personal data. As Pobal supports vulnerable groups, the questions can be a barrier for the participants to participate in the programmes. Moreover, as there is no specific end data for engaging in the programmes, it is hard to collect exit and re-engaging

[551] Interview, Department of Social Protection 1 (Intermediary body for Aid to the Most Deprived, Ireland), 14 November 2022.

[552] Interview, Department of Social Protection 2 (Intermediary body, Back to Work Enterprise Allowance scheme), 21 November 2022.

[553] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[554] Interview, HEA- Higher Education Authority (Intermediary body, Ireland), 16 November 2022.

[555] Interview, HEA- Higher Education Authority (Intermediary body, Ireland), 16 November 2022.

[556] Interview, HEA- Higher Education Authority (Intermediary body, Ireland), 16 November 2022.

data. Therefore, Pobal is exploring the use of representative sampling to reduce administrative burden regarding the collection of data regarding long-term results[557].

Potential solutions/good practices

- When working on the European Globalisation Adjustment Fund (EGF) regarding unemployed workers, PEIL was able to get data on employment updates every four months from the Revenue Commissioners to meet EGF reporting requirements, which is not as detailed as ESF reporting requirements. The managing authority has tried to renew this. If an ESF scheme were to be solely focused on employment, PEIL would potentially be able to get all missing (i.e., employment outcome) monitoring data from the Revenue Commissioner. It would make it easier to work on a data sharing agreement early during the ESF programmes to enable proper monitoring and evaluation[558].

- During the programme, the data protection advisors of the intermediary bodies suggested that the legal requirement to collect data should be based on the regulations or the basis of significant public interest to process data. That would facilitate greater use of existing data rather than looking for explicit consent[559].

- A data protection contact point for the ESF would be useful. Within the Erasmus programme, there are very useful guidelines on data processing and GDPR[560].

Guidance/advice

- The government's legal team (Chief State Solicitor's Office), the Attorney General's office, has given advice on data sharing agreements on processing the sharing of data but not on the use of administrative records. They advised to seek explicit consent. However, the data protection advisors of the intermediary bodies suggested instead that justification of data collection should be based on the legal obligation to collect data (Article 6(1)(c) GDPR) or the basis of significant public interest (Article 6(1)(e) GDPR) to process data. That would facilitate greater use of existing data rather than looking for explicit consent, according to the managing authority[561].

- The department of Social Protection has internal DPOs who train staff on GDPR and who have knowledge of ESF, so there is no need for additional advice[562].

- At the HEA, an internal DPO is involved in the process, and DPOs at the parent organisation has also been consulted. The auditors are also involved. The HEA

[557] Interview, Pobal (Beneficiary SICAP, Ireland), 10 November 2022.

[558] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[559] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[560] Interview, HEA- Higher Education Authority (Intermediary body, Ireland), 16 November 2022.

[561] Interview, PEIL (managing authority, Ireland), 12 October 2022.

[562] (1) Interview, Department of Social Protection 1 (Intermediary body for Aid to the Most Deprived, Ireland), 14 November 2022. (2) Interview, Department of Social Protection 2 (Intermediary body, Back to Work Enterprise Allowance scheme), 21 November 2022. (3) Interview, Department of Social Protection 3 (Intermediary body, JobPlus Youth scheme), 21 November 2022.

review the process continuously with the auditors. In the future, it might be useful to also involve DPOs from the beneficiaries[563].

- For the beneficiary WAP, guidelines come from the Department of Rural and Community Development, and Pobal. The guidelines work and are quite simple. However, additional guidance may be needed regarding ownership of the data fed into the database that they use. The ownership status is quite vague regarding if WAP is the owner or user of data, as it uses a national database. The Department of Rural and Community Development, and Pobal, should give better clarity as they cannot answer who is the data controller and who is the processor, etc[564].

- The beneficiary Pobal has received advice and guidance from an in-house DPO which has been helpful and has undertaken a risk assessment[565].

8.3.5. Italy

Types of data collected and used

Innovazione Apprendimento Lavoro (IAL) Friuli Venezia Giulia (FVG), an ESF beneficiary that conducts education and training, collects information from participants that include biographical information, address, e-mail address, Tax ID, education, and degrees achieved, employment status, and sector employed. Collect is done via the regional FP1-B registration form, completed, signed and with an ID document attached. If the course is online, there is a simplified form, including a consent form[566]. Note that this information is mentioned by one beneficiary only, that is implementing education and training courses, so other beneficiaries may collect other types of information.

In Italy, administrative data are used for both monitoring and evaluation[567]. For monitoring and evaluation purposes, ANPAL, a national ESF managing authority, collects employment data regarding participants, and tax, police, and court records regarding beneficiaries[568]. The Marche Region, a regional ESF managing authority, mentioned that monitoring data from the JOB Agency data base is linked through a unique identifier, the Italian fiscal code, a tax code. For evaluation purposes, the Marche Region also uses data from the COMarche dataset that includes information on sex, age, education, citizenship, and employment history. Also, the ASIA dataset is used, which contains enterprise information about sector, number of employees, and data of birth[569].

The Ministry of Economy and Finance (MEF) General Inspectorate for Financial Relations with the European Union (IGRUE) manages the national monitoring system, a database for implementing the cohesion policies. Managing authorities are required to submit to this database every second month, through their local information systems, information on physical, financial, and procedural progress of financed projects. However, this information does not necessarily contain personal information[570].

[563] Interview, HEA- Higher Education Authority (Intermediary body, Ireland), 16 November 2022.

[564] Interview, WAP - Waterford Area Partnership (Beneficiary, Ireland), 15 November 2022.

[565] Interview, Pobal (Beneficiary SICAP, Ireland), 10 November 2022.

[566] Interview, Innovazione Apprendimento Lavoro Friuli Venezia Giulia (ESF Beneficiary, Italy), 26 October 2022.

[567] Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 03 November 2022.

[568] Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 03 November 2022.

[569] Interview, Marche Region (ESF managing authority, Italy), 21 October 2022.

[570] Interview, Ministry of Economy and Finance – IGRUE (Administrative Data Holder, Italy), 26 October 2022.

Storing data

One concrete example on how data are stored in Italy comes from the interview with the ESF beneficiary IAL FVG. They have their own internal digital management system, Ial Man, which records and makes available all data needed to implement the ESF projects. They rely on a datacentre storage that is based in Milan, and which handles all back-ups and security solutions[571]. Moreover, the managing authority ANPAL described that they use an internal database to store administrative data, which can be accessed freely by authorised employees[572].

Transferring data

Transferring participants' personal data

As described above, the information that is collected about participants can include biographical information, address, e-mail address, Tax ID, education, degrees achieved, employment status, and sector. This information is transferred to the FVG Region for monitoring and reporting purposes[573].

Transferring administrative data

A national monitoring system is used by the MEF IGRUE to transfer non-personal data to the European Commission and publicly display information on key financial indicators at the monitoring system's website. Also, information is transferred to other public institutions such as the Italian National Institute of Statistics (ISTAT), the Bank of Italy, and the Italia Court of Auditors[574].

IAL FVG, who collects information directly from ESF project participants, can also access personal information from other organisations through an interoperability system which allows the "job canters" to digitally transfer the user's data to the operators in charge of professional education within the Region[575].

The managing authority ANPAL has special agreements in place according to data protection rules to access the administrative data required from other public institutions[576]. Also, and as mentioned above, the managing authority of the Marche Region can gain access to several administrative datasets, both for monitoring and evaluation purposes[577]. To external evaluators, data may be provided anonymised to evaluators, but not always. If the data comes non-anonymised, they are followed by privacy rule protocols, and may only include sub-samples of variables[578].

[571] Interview, Innovazione Apprendimento Lavoro Friuli Venezia Giulia (ESF Beneficiary, Italy), 26 October 2022.

[572] Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 03 November 2022.

[573] Interview, Innovazione Apprendimento Lavoro Friuli Venezia Giulia (ESF Beneficiary, Italy), 26 October 2022.

[574] Interview, Ministry of Economy and Finance – IGRUE (Administrative Data Holder, Italy), 26 October 2022.

[575] Interview, Innovazione Apprendimento Lavoro Friuli Venezia Giulia (ESF Beneficiary, Italy), 26 October 2022.

[576] Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 03 November 2022.

[577] InterviewMarche Region (ESF managing authority, Italy), 21 October 2022.

[578] Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 03 November 2022.

Using and linking data

Data gathered, directly from participants and administrative data, are used for both monitoring and evaluation purposes.

MEF IGRUE uses the national monitoring system mainly for financial reporting and to analyse activities carried out by other public institutions[579].

The managing authority of the Marche Region uses several administrative datasets for evaluation purposes. For example, the JOB Agency administrative dataset is used to calculate the gross employment rate of participants. It is done to calculate the ESF operational Programme indicator on participants in employment, including self-employed, six months after leaving, and the long-term employment indicator. Monitoring data collected from ESF participants is linked to the JOB Agency dataset through a unique identifier in the form of a tax/social security number to assess unemployment durations, and for impact analyses using counterfactual methods[580].

Challenges

The managing authorities ANPAL and of the Marche Region did not mention any crucial challenges related to accessing administrative data. However, it is not always possible to access complete datasets requested[581]. Moreover, ANPAL described it potentially being a challenge to comply with both EU and national data protection legislation, especially data processing regarding GDPR Articles 9 and 10. Another challenge concerns the interconnection between different information systems[582].

The beneficiary IAL FVG mentioned that they do not face any challenges regarding data protection. However, one challenge concerns a lack of interoperability between regions and the national level[583].

Potential solutions

Certain data protection restrictions might be overcome through an impact assessment of data processing pursuant to Article 36 of the GDPR and a possible consultation with the National Supervisory Authority[584].

Guidance/advice

The Italian interviewees did not mention much regarding DP advice, and when advice is given, it generally comes internally. ANPAL got internal advice regarding guidelines from the EDPB but is open to additional advice concerning public administrations' processing of

[579] Interview, Ministry of Economy and Finance – IGRUE (Administrative Data Holder, Italy), 26 October 2022.

[580] Interview,Marche Region (ESF managing authority, Italy), 21 October 2022.

[581] Interview, Marche Region (ESF managing authority, Italy), 21 October 2022.

[582] Interview, Innovazione Apprendimento Lavoro Friuli Venezia Giulia (ESF Beneficiary, Italy), 26 October 2022.

[583] Interview, Innovazione Apprendimento Lavoro Friuli Venezia Giulia (ESF Beneficiary, Italy), 26 October 2022.

[584] Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 03 November 2022.

personal data[585]. Moreover, IAL FVG has an internal supervisory body that implements a system for monitoring and reporting, including a proper use of data. However, although it might be useful to have a control system in place, it has never been necessary to use it. In general, IAL FVG, mentions that the system is sufficient as it is, and that no additional advice is currently needed[586]. Beside these examples, MEF-IGURE has not received any advice but mentions that guidance could potentially be useful[587].

The Italian DPA has not formally provided any guidance regarding ESF or carried out any investigation. However, the authority has been in contact with several national authorities and the European Data Protection Supervisor regarding transmission of ESF beneficiaries' personal data (other than those referred to in Articles 9 and 10 of the Regulations) to the managing authorities for the purposes of monitoring, evaluation, financial management, verification, and auditing under Regulation (EU) 1303/2013. It concerned state payments on redundancy benefits under exceptional circumstances and was grounded in the obligation for the managing authorities to record and store data on each operation, including data on individual participants in operations, where applicable pursuant to Article 125(2)(d) of Regulation (EU) 1303/2013. As for the accounting of the expenditure supported by the ESF, this regulation requires the managing authorities to provide the audit authority with accounting records for that expenditure for the purpose of carrying out the audit activities referred to in Article 127(1) as well as to provide supporting documents regarding such expenditure to the European Commission upon request pursuant to Article 140(1). In this regard, by way of its decision No 275 of 17 December 2020[588], the IT SA ordered 'the controllers involved in the data transmission at issue to consider implementing pseudonymisation techniques with regard to the beneficiaries' Tax IDs' and requested the public body concerned to inform the DPA about the assessment and measures taken "by including adequate supporting evidence, where appropriate, as to the reasons why the pseudonymisation of beneficiaries' Tax IDs would prevent the achievement of the purposes of the processing as pursued from time to time'. This case highlights the importance of complying with data protection principles, and in particular the data minimisation principle, when processing personal data in connection with monitoring, evaluation and audit activities under the aforementioned regulation[589].

Additional information

With specific regard to guidance on the reuse of public sector datasets - including personal data - by another public authority, on 15 May 2014, the Italian DPA issued general guidelines[590] for the processing of personal data, as also contained in administrative records and documents, carried out by public bodies for the purposes of publicity and transparency on the web. Section 6 of those Guidelines addresses the 'reuse' of personal data as envisaged by the provisions of the Legislative Decree No 33/2013[591].

Moreover, on 26 August 2021, the DPA delivered a favourable opinion[592] on the draft legislative decree containing 'Implementation of Directive (EU) 2019/1024 on open data and the reuse of public sector information (recast)' along with some recommendations inviting

[585] Interview, ANPAL - Agenzia Nazionale Politiche Attive Lavoro (ESF managing authority, Italy), 03 November 2022.

[586] Interview, Innovazione Apprendimento Lavoro Friuli Venezia Giulia (ESF Beneficiary, Italy), 26 October 2022.

[587] Interview, Ministry of Economy and Finance – IGRUE (Administrative Data Holder, Italy), 26 October 2022.

[588] Available on the website of the DPA at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9519360.

[589] Interview, The Italian Data Protection Authority, 03 November 2022.

[590] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/3134436.

[591] https://www.normattiva.it/eli/id/2013/04/05/13G00076/CONSOLIDATED/20221118.

[592] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9717493.

the government to consider including a few amendments to the draft Decree in order to further put it in line with the data protection rules and principles.

The abovementioned guidelines originated from the adoption of relevant changes to the national legislative framework on the transparency of public administrative bodies (Legislative Decree No. 33/2013). Those changes made it necessary for the Italian DPA to step in to ensure compliance with the rules and principles on the protection of personal data applicable to public bodies in the face of the web-based publication obligations arising from the new legislative framework. The guidelines aim to identify appropriate measures and safeguards public bodies are required to implement whenever they disseminate personal data on their official websites for transparency purposes or for other purposes related to publicity of administrative activities. Considering the different applicable legal regimes, the guidelines distinguish the publication obligations for transparency purposes from the publication obligations for other purposes (e.g., legal publicity).

As noted above, Section 6 of the guidelines addresses the 'reuse' of personal data as envisaged by the provisions of Legislative Decree No 33/2013. Those provisions envisage that information, documents and data falling within the scope of the mandatory publication requirements under the said Legislative Decree are re-usable in compliance with the national law on the protection of personal data as well as the national law implementing the Directive (EU) 2019/1024 on open data and the reuse of public sector information (Legislative Decree No 36/2006[593]). In this regard, the Guidelines highlight that the amended Directive (EU) 2019/1024 reaffirms the principle that the reuse of public sector information is without prejudice to the protection of individuals with regard to the processing of personal data under EU and national law. Indeed, the Directive introduces specific exceptions to the reuse of public sector information based on data protection reasons and provides that certain public sector documents containing personal data are excluded from the rules on the reuse even if they are freely accessible online.

This means, inter alia, that the reuse of personal data made publicly available online by public bodies pursuant to the transparency obligations of Legislative Decree No 33/2013 is not permitted "if it is in any way incompatible" with the original purposes for which the said data were made publicly available - in line with the data protection principle of purpose limitation. Therefore, in order to avoid losing control over the personal data published online and to reduce the risks of their inappropriate use, the Guidelines recommend that public bodies subject to publication obligations under Legislative Decree No 33/2013 include an alert in their official websites informing the public that the personal data published therein are "reusable only under the conditions provided for by the legislation on the reuse of public sector information in a way that is compatible with the purposes for which they were collected and recorded, and in compliance with the legislation on the protection of personal data".

Moreover, when taking decisions on the scope and conditions for the reuse of public sector documents containing personal data, public bodies have to carry out a data protection impact assessment in accordance with Article 35 of the GDPR so as to reduce the risk of losing control over the data or having to deal with requests for damages from the data subjects. Regarding the impact assessment, it must be taken into account that special categories of personal data and judicial personal data are expressly excluded from the scope of reusable public sector information according to the applicable law on transparency of public administrative bodies (see Section 7-a of Legislative Decree No 33/2013).

[593] https://www.normattiva.it/eli/id/2006/02/14/006G0046/CONSOLIDATED/20221118.

8.3.6. Poland

Types of data collected and used

ESF participant data

The evaluator OpenField stated that they access participant data such as name, address, e-mail, phone number, gender, date of birth, and employment status[594]. The provincial office of Warsaw collects similar basic data, and for some programmes, additional 'sensitive' data may be collected such as regarding homelessness or addictions. These types of data are optional, and the beneficiaries do not have to provide them[595].

Administrative data

Several administrative databases were mentioned to be in use for both monitoring and evaluation of ESF projects and programmes[596]. These include the SYRIUSZ system that is managed by the Ministry of Labour, which contains, e.g., labour- and education- related data. Also, the National Official Register of the Territorial Division of the Country (TERYT) database, run by the Central Statistics Office, is being used to verify ESF data. It contains information such as on municipalities and addresses. Moreover, the Ministry of Funds and Regional Development use data from the Social Insurance Agency regarding paid insurance contributions to calculate long-term result indicators, and the Central Examination Commission to evaluate support given through the operational programme Knowledge, Education and Development.

Overall ESF-related data management system, including transferring and accessing participants' and administrative data

In Poland, the supervision and monitoring of the implementation of projects co-financed by the ESF is currently within the scope of responsibility of the Minister of Family and Social Policy. As part of these responsibilities, the authorised entity has access to, among others: accounting documents, including invoices, bills, accounting notes, payrolls and concluded contracts. Documents subject to the control of the Minister of Family and Social Policy may contain personal data[597]. However, other actors interviewed did not mention any access to these data.

The evaluator OpenField explains that they obtain data from data administrators, which in most cases are administrative regional authorities. They collect such data from organisations which implement ESF programmes. These organisations collect data from ESF beneficiaries and enter the data into the "SL" database. Each region is an administrator

[594] Interview, OpenField (Evaluator, Poland), 20 October 2022.

[595] Interview, Employment Office of the Capital City of Warsaw (Administrative data holder, Poland), 27 October 2022.

[596] (1) Interview, Ministry of Funds and Regional Development (managing authority, Poland), 31 November 2022. (2) Interview, Employment Office of the Capital City of Warsaw (Administrative data holder, Poland), 27 October 2022. (3) Interview, OpenField (Evaluator, Poland), 20 October 2022.

[597] Interview, Office for Protection of Personal Data (Poland), 14 November 2022.

of such a database on a regional level. The Ministry of Funds and Regional Development consolidates these databases for the whole country[598].

The SL database is a sub-database to- and integrated with another database called SYRIUSZ. The SYRIUSZ database consists of unemployment data and ESF participants' data from previous projects. Data is entered in here by Employment Offices throughout the country. After completion of ESF-funded projects, data on project participants are entered into the SYRIUSZ and SL databases to enable the tracking of unemployed persons and their participation in various projects[599].

The Ministry of Funds and Regional Development stated that the SYRIUSZ system will be similar in the current ESF+ funding period. Each regional labour authority will feed the SYRIUSZ with information about age, experience, education, support provided, employment status, and related expenses. In terms of monitoring, the use of data from the SYRIUSZ system greatly facilitates the process of verifying the data of ESF and ESF+ project participants and avoids collecting the same information twice from a given person[600].

To access data from the Social Insurance Agency, the Ministry of Funds and Regional Development had to sign a special agreement. In general, such agreements are necessary to access administrative data from different institutions. Internally, all personal data processing activities undertaken for which the Ministry is the controller, are supervised by the controllers located in the individual departments of the Ministry[601].

At a regional level, the Employment Office of the Capital City of Warsaw must have a special legal basis for accessing data from the regional administrative employment office[602].

From the evaluator's perspective, OpenField receives data from the SYRIUSZ and SL databases via e-mail and get a password in a separate e-mail to access the files. One employee is responsible for the preliminary processing of the database and, if needed, for dividing it into smaller fragments which are then distributed to other employees, who process the data relating to a specific assignment. There are specific routines and procedures according to contracts with clients and internal protocols. Only persons who analyse the specific data have access to these, and the data are destroyed after the end of each contract. Moreover, data is stored on servers in the company and access to the company offices is secured with alarm doors. Someone working from home would not be able to access this data[603].

Challenges and solutions

Challenges mentioned among the interviewees refer to legal restrictions, time-consuming procedures, and interoperability of data systems. The Ministry of Funds and Regional Development mentioned that it can take several years to conclude data sharing agreements to facilitate access to administrative data. In addition, it can be costly and time-consuming to extract data from registers and adapt IT systems to process the data. These challenges relate mostly to processes required for data necessary for evaluations. Therefore, the

[598] Interview, OpenField (Evaluator, Poland), 20 October 2022.

[599] Interview, Employment Office of the Capital City of Warsaw (Administrative data holder, Poland), 27 October 2022.

[600] Interview, Ministry of Funds and Regional Development (managing authority, Poland), 31 November 2022.

[601] Interview, Ministry of Funds and Regional Development (managing authority, Poland), 31 November 2022.

[602] Interview, Employment Office of the Capital City of Warsaw (Administrative data holder, Poland), 27 October 2022.

[603] Interview, OpenField (Evaluator, Poland), 20 October 2022.

ministry calls for increased legal flexibilities for the application, use, and transfer of administrative data between public authorities[604].

The polish data protection law prescribes that entities which process personal data must have special procedures in place for handling a large volume of personal data. However, the legislation does not describe specific procedures for data protection which results in different legal interpretations. Therefore, it can be complicated and costly to understand the necessary rules and procedures. The evaluator OpenField suggests having specific rules in place to allow clear and uniform approaches[605].

Guidance/advice

No interviewee has got any advice from the Data Protection Office. This is confirmed by the Data Protection Office themselves, who has had no interaction regarding ESF-related matters. Instead, the actors interviewed make use of either internal DPOs or contract external companies for data protection advice. The Ministry of Funds and Regional Development has controllers in each department, and DPOs are involved on more complicated cases such as complaints. Such cases concern evaluation data and not monitoring data which is easier to process[606]. Moreover, the Ministry of Funds and Regional Development provides rules for, e.g., evaluators such as OpenField, who also contract data protection inspectors to prepare all procedures[607]

As stated above, the Polish Data Protection Office has not been involved in any ESF-related matters or formulated specific guidelines. However, the interviewee thought it worth noticing a number of related considerations[608]:

Pursuant to Article 69 sec. 1 of the Act of 11 July 2014 on the rules for the implementation of cohesion policy programmes financed under the 2014-2020 financial perspective (Journal of Laws of 2020, item 818, as amended), an ICT system was created to support the implementation of Operational Programmes, including those supported from the ESF. This system serves, among others, to support processes related to evaluation (Article 69(3)(4) of the aforementioned Act). On October 26, 2022, our Office submitted comments to the draft act on employment activities. This draft (Article 44) envisages creation of an ICT system containing a central register of personal data of natural persons applying for assistance specified in this Act or persons using this assistance and other persons. The provisions of the draft act also apply to the beneficiaries of the ESF. More on this in Section 6 below. (DP Office, PL)

According to Article 44 item 2 of the draft act on employment activities, the minister competent for labour matters processes personal data of natural persons in the central register in order for public employment services to perform statutory tasks, including verification of entitlements and data, registration and determination of status, providing assistance specified in the act, issuing decisions in terms of status and benefits, conducting control proceedings, fulfilling reporting obligations and obligations in the field of official statistics, and defining plans for further action.

According to this draft Act, personal data are to be processed in the register, including the unemployed, job seekers, foreigners intending to work in the territory of the Republic of

[604] Interview, Ministry of Funds and Regional Development (managing authority, Poland), 31 November 2022.

[605] Interview, OpenField (Evaluator, Poland), 20 October 2022.

[606] Interview, Ministry of Funds and Regional Development (managing authority, Poland), 31 November 2022.

[607] Interview, OpenField (Evaluator, Poland), 20 October 2022.

[608] Interview, Office for Protection of Personal Data (Poland), 14 November 2022.

Poland, entrepreneurs, and insured persons. Huge amounts of personal data are to be processed in the register.

The project team negatively assessed the plan to create the above-mentioned ICT system, indicating, among others, that the project promoter creates a centralised database - a huge amount of personal data - in which a significant amount of personal data will be processed, including data of special categories, previously processed in separate registers (voivodeship employment offices, poviat employment offices, registers of accredited entities), as well as from natural persons applying for the assistance specified in the draft act. In our opinion, the direction taken by the creator of the act is in contradiction to the rules on the processing of personal data resulting from Regulation 2016/679 (GDPR). It is also inconsistent with the case law of the CJEU in this regard (cf. judgment in case C-201/142 Sandra Bara et al.)

8.3.7. Romania

Types of data collected, accessed, used, and how

ESF participant data

If personal data are collected directly from participants, a consent form is used. The type of data collected depends on the context of the research, but may include, e.g., gender, level of education, civil status, income, and employment status[609].

Administrative data

A researcher at the University of Bucharest, an ESF beneficiary, has most frequently used data from public sources, but also from school or education records/registers[610].

Two ESF/ESF+ managing authorities were interviewed, and only one of them uses administrative data. For Evaluation purposes, it uses data on employment status, job seekers, and beneficiaries utilising unemployment services, including training. For monitoring purposes, it uses data from[611]:

- Employment records (General Registry of Employees, Labour Inspection)
- The National Agency for Fiscal Administration such as income and social contributions
- The National Agency for Unemployment, including information on trainings that beneficiaries have participated to at the Agency
- The National House of Public Pensions
- The Trade Register Office

[609] Interview, University of Bucharest (Beneficiary, Romania), 24 October 2022.

[610] Interview, University of Bucharest (Beneficiary, Romania), 24 October 2022.

[611] Interview, National Unemployment Agency (managing authority, Romania).

- National Agency for Social Benefits regarding minimum social income.

The National Unemployment Agency explained that it processes personal data only for defined purposes. To access data, one must define the purpose. Moreover, it said that the procedure for gaining access would differ depending on the processing purpose and category of personal data. Also, the data can be accessed at different frequencies depending on the importance of the service[612].

If administrative data contain personal information, the managing authority UEFISCDI explained that to access such data, an institution needs to comply with the following requirements[613]:

- Be an authorised institution that can work with personal data.
- Have clear legal provisions regarding the legal right to access that information.
- Have a clear protocol between the institution that provides the administrative data and the institution.
- Clearly define the persons that have the right to use that data. (UEFISCDI, MA, RO).

While the other interviewees seemed to have access to, and/or be able to share personal and administrative data, the national statistical institute said that it is not allowed to do so. The institute is bound by confidentiality by law, both European and national law: Reg. (EC) 223/2009 and Law 226/2009 on the organisation and operation of official statistics in Romania. Data are considered confidential when they make it possible to identify a statistical unit (natural or legal person). As a result, official statistics are made available to everyone through aggregated statistical data in the form of statistical indicators. Laws on the processing of personal data for statistical purposes under the GDPR, along with statistical confidentiality, require the existence of safeguards by which the necessary technical and organisational measures have been established to prevent any unauthorised dissemination[614].

Challenges

- Restricted access to data on education (handled by the Ministry of Education), due to insufficient clarification on the legal basis for processing such information[615].
- Lack of transparency, lack of collaboration between institutions, and lack of coherent procedures and regulations. Also, the cost to access data can be an issue[616].
- Legal processing (Article 6 of GDPR) requires better regulation in Romania (public interest, legal obligation[617].

[612] Interview, National Unemployment Agency (managing authority, Romania).

[613] Interview, UEFISCDI (managing authority, Romania).

[614] Interview, The Romanian National Statistical Institute, 28 October 2022.

[615] Interview, National Unemployment Agency (managing authority, Romania).

[616] Interview, University of Bucharest (Beneficiary, Romania), 24 October 2022.

[617] Interview, National Unemployment Agency (managing authority, Romania).

Potential solutions/good practices

- Since one must define the purpose of data processing to access data, a better description of purposes would be useful. Also, it would be useful to elaborate clear eligibility rules, so it is no longer necessary to verify the entire documentation containing personal data[618].

Guidance/advice

The interviewee from the National Unemployment Agency was the only one who stated having received advice from the National DPA. To get advice, the agency requested the authority's view on processing information related to education regarding the possibility of concluding a protocol with the Ministry of Education for communicating such data to the Unemployment Agency. The authority replied that the Romanian legislation must be aligned to the requirements imposed under the GDPR and, thus, clarify the legal basis for communicating information regarding education to the Unemployment Agency. Thus, a protocol cannot constitute a legal basis for data processing. Moreover, the agency would need additional advice and clarification on the legal basis and purpose of processing personal data for administrative purposes[619].

The National DPA answered in an interview that it constantly had interaction with national authorities that process personal administrative data for various purposes, by issuing opinions on the processing of personal data, in general, according to the applicable legal framework, but not specifically related to the ESF monitoring and/or evaluation purpose[620].

8.3.8. Spain

Types of data collected and used

ESF participant data

Interviewees did not mention specific information that is being collected form participants to a large extent. Information can include age, gender, education, and employment[621]. In general, data include figures on the employment or education situation of the participants as well as data disaggregated by gender. In no case, neither special categories of personal data nor microdata of individual persons are handled due to data protection law. To handle special categories of personal data, consent is required from everyone. The steps to obtain data for the purpose of monitoring or evaluation reports are usually surveys, interviews, and other consultations[622].

[618] Interview, National Unemployment Agency (managing authority, Romania).

[619] Interview, National Unemployment Agency (managing authority, Romania).

[620] Interview, The National Supervisory Authority for Personal Data Processing (Romania), 14 December 2022

[621] Interview, Red2Red (evaluator, Spain), 19 October 2022.

[622] Interview, UAFSE - Spanish Administrative Unit of the European Social Fund (managing authority, Spain), 15 November 2022.

Administrative data

To select participants, one beneficiary mentioned that data on workers registered with the national and regional public employment services are being used. Also, data are used from the national Tax Administration Agency regarding date of birth and economic situation, and social security registers for information regarding possible vulnerable situations such as social service programmes situations of gender-based violence. To access most of these data, it requires consent from the individuals involved[623].

Another beneficiary mentions similarly that they can access a wide range of administrative data. These include name, ID, social security number, address, phone number, academic and professional background, bank details, and financial data such as payroll, credits, loans, guarantees, and judicial withholdings if applicable. The information can be used for a range of different purposes for all services provided directly or indirectly by the beneficiary[624].

ESF/ESF+ managing authorities and evaluators, whether external or not, use the databases of the Public Employment Services and the Ministry of Education to report and inform the employment and education situation of programme participants[625].

According to Red2Red, evaluators can only use data that is necessary for the evaluation, both socioeconomic data such as regarding age, education, employment, and gender, and monitoring data such as number of people involved in specific actions. The kind of information accessed and used is what is referred to in the ESF regulation. Types of data include public register data (births, marriages, and deaths), immigration records, employment status, school or education records, and social services records. The only additional information comes from the Spanish social security health system. Since other kind of data or special categories of personal data cannot be used for evaluation, it is hard to make holistic assessments[626].

Transferring and accessing data

Transferring participants' personal data

According to the national managing authority UAFSE, data collection for the purpose of monitoring and evaluating ESF programmes is decentralised to autonomous communities and regional authorities as they act as intermediary bodies. These data are provided to UAFSE aggregated. All the managing authorities and evaluators, whether external or not, use the databases of the Public Employment Services and the Ministry of Education to report and inform on the employment and education situation of programme participants[627].

Accessing, transferring, and using administrative data

[623] Interview, Mancomunidad Intermunicipal Alto Palancia (Beneficiary, Spain), 04 November 2022.

[624] Interview, UCM - General Foundation of Universidad Complutense de Madrid (Beneficiary, Spain), 08 November 2022.

[625] Interview, UAFSE - Spanish Administrative Unit of the European Social Fund (managing authority, Spain), 15 November 2022.

[626] Interview, Red2Red (evaluator, Spain), 19 October 2022.

[627] Interview, UAFSE - Spanish Administrative Unit of the European Social Fund (managing authority, Spain), 15 November 2022.

Reuse of administrative data by public institutions is widely covered in Spanish legislation[628]. Regarding ESF, administrative data is used for both identifying project participants and for monitoring and evaluating performance.

Administrative data that is used to identify ESF project participants can be gained from different institutions such as public employment agencies and the tax agency[629].

Monitoring and evaluation are reported annually in an annual implementation report per programme, which use the aggregated data that are provided by the intermediary bodies. Thematic evaluations are normally carried out by external contractors under the supervision of the managing authority UAFSE. The methodology to attain data is indicated in each evaluation. Type of data and data source vary depending on the programme and its purpose[630]. To access administrative data for the purpose of monitoring and evaluating ESF programmes, the interested party must comply with certain legal criteria and security requirements[631].

As stated above, the evaluator Red2Red accesses data from several different regional and national public institutions. They can access data that is necessary according to the ESF regulation from, e.g., immigration, employment, education, and social service records. For each evaluation, special agreements are made, and there is in general no restrictions if the rules are followed. However, the data provided are not sufficient to address success rates[632].

The regional statistics institute in Valencia stated that the regional statistics institutes, except for those in Catalonia and the Basque Country, use only fully anonymised data from the National Statistics Institute. Some public administrations provide them only exceptionally with basic personal data such as ID card number, employment history, health records, and income level[633].

Challenges

Different interviewees mentioned different types of challenges related to accessing and using administrative data for the purpose of monitoring or evaluating the ESF. These include the lack of data, data protection restrictions to access existing data, time-consuming processes to access these data, a lack of interoperability between administrative data holders, and restrictions on using the data.

The evaluator Red2Red stated that there is a general problem regarding the lack of existing data in terms of public authorities' inability to collect data. In addition, not all data that are needed for comparison are available for evaluators. For example, there are DP challenges to access data on employment. Partly because employment data is considered a special category of personal data. Another challenge concerns the time it takes to get hold of administrative data. For example, if one needs to get hold of anonymised data, it takes a long time to get these anonymised[634].

[628] Interview, Spanish Data Protection Agency, 18 October 2022.

[629] Interview, Mancomunidad Intermunicipal Alto Palancia (Beneficiary, Spain), 04 November 2022.

[630] Interview, UAFSE - Spanish Administrative Unit of the European Social Fund (managing authority, Spain), 15 November 2022.

[631] Interview, UCM - General Foundation of Universidad Complutense de Madrid (Beneficiary, Spain), 08 November 2022.

[632] Interview, Red2Red (evaluator, Spain), 19 October 2022.

[633] Interview, Statistical Institute (Region of Valencia, Spain), 28 October 2022.

[634] Interview, Red2Red (evaluator, Spain), 19 October 2022.

One challenge concerns differences between regions and levels of governments and the lack of coherence in how administrative data is processed. The interviewee of the beneficiary Mancomunidad Intermunicipal Alto Palancia stated that although there are no difficulties in accessing or using administrative data, there is a lack of interoperability between different administrative data holders which creates inefficiency in data processing[635]. Moreover, there are also differences between regions. According to the evaluator Red2Red, data processing is more efficient in the Basque Country or Catalonia compared to other regions and at national level[636].

Public statistical institutes seem to face other challenges concerning administrative data. According to Eustat, data protection regulation is very strict in Spain regarding data for statistical purposes. Public statistical institutes in Spain such as Eustat have access to multiple types of data from different sources. However, they are not allowed to use all or share them due to data protection legislation and statistical secrecy rules. Data is only shared in anonymised and aggregated form. Moreover, the statistical institutes cannot process any personal data to carry out ESF evaluations[637].

Potential solutions/good practices

Related to the challenges above, there should be greater data processing coherence between regions and levels of government and better interoperability between the systems. As a solution, the beneficiary Mancomunidad Intermunicipal Alto Palancia mentioned that access to the Spanish Government's Data Intermediation Platform would facilitate greater interoperability. However, it is hard to join this platform due to IT and staff issues[638].

Other suggestions concern types of data that should be possible to access to better facilitate evaluations and ways to facilitate more access to administrative data. For example, the evaluator Red2Red suggested that to facilitate evaluations, public register data should be linked to tax register data such as income level. Moreover, it mentioned two good practices: an agreement made between the managing authority UAFSE and a Spanish consultancy and the system in Catalonia to provide data to consultancies[639].

The beneficiary Mancomunidad Intermunicipal Alto Palancia suggested two improvements. First, since accessing administrative data requires consent from data subjects, consent should be collected in advance. Second, the county council should provide more data protection guidance[640].

In the Basque Country, the public administration has a large amount of information available to the Basque Institute of Statistics. However, these are governed for statistical purposes and not research purposes, which is a difference that implies that research administrations benefit from exceptions in the processing of personal data, exceptions that are not applicable to statistical institutes. In Spain, statistical institutes are autonomous bodies with a legal personality and their own assets. However, these are dependent on the national or autonomous governments. According to Eustat, it would be convenient to differentiate between public purposes (of any type of administration) and private ones instead of

[635] Interview, Mancomunidad Intermunicipal Alto Palancia (Beneficiary, Spain), 04 November 2022.

[636] Interview, Red2Red (evaluator, Spain), 19 October 2022.

[637] Interview, Eustat (Statistical Institute, Basque Country, Spain), 16 November 2022.

[638] Interview, Mancomunidad Intermunicipal Alto Palancia (Beneficiary, Spain), 04 November 2022.

[639] Interview, Red2Red (evaluator, Spain), 19 October 2022.

[640] Interview, Mancomunidad Intermunicipal Alto Palancia (Beneficiary, Spain), 04 November 2022.

statistical and research purposes to reduce widespread restrictions on the processing of personal data[641].

Guidance/advice

The Spanish Data Protection Agency (AEPD) stated that it has not been involved in any ESF-specific issues. It has not been in contact with the Administrative Unit of the European Social Fund (AUESF) in Spain but with other authorities continuously[642]. Indeed, the beneficiary UCM referred to several recommendations, guidelines, and documents that specify how to process personal data but pointed out that there are no proactive measures implemented by the AEPD that describe and specify how to process and manage different kinds of data in the context of ESF[643]. Several interviewees stated that specific guidance would be useful, both nationally and regionally from regional data protection authorities.

The evaluator Red2Red thinks that there is a general lack of data protection guidance from the AEPD. Proactive advice at national and regional level would be crucial to lawfully provide statistical information and other personal data[644]. Eustat believes similarly that support from the Basque DPA and the Spanish Agency for Data Protection has been insufficient[645].

Since the Valencian Community has no regional DPA, the Valencian statistical institute relies on AEPD. The Valencian statistical institute believes that AEPD should implement more guides and guidelines to create a greater typology of data in coherence with data protection regulations to facilitate more precise and reliable statistics[646].

An explanation of Spanish data protection legislation and references to relevant guidance documents are available in the interview summary of the interview with the Spanish Data Protection Agency.

8.3.9. Sweden

Types of data collected, shared, and or used

ESF participant data

- Personal data, including special categories of personal data[647].
- Name, social security number, employment status, qualifications achieved, participation in ESF activities[648].

[641] Interview, Eustat (Statistical Institute, Basque Country, Spain), 16 November 2022.

[642] Interview, Spanish Data Protection Agency, 18 October 2022.

[643] Interview, UCM - General Foundation of Universidad Complutense de Madrid (Beneficiary, Spain), 08 November 2022.

[644] Interview, Red2Red (evaluator, Spain), 19 October 2022.

[645] Interview, Eustat (Statistical Institute, Basque Country, Spain), 16 November 2022.

[646] Interview, Statistical Institute (Region of Valencia, Spain), 28 October 2022.

[647] Interview, Arbetsförmedlingen (Beneficiary and administrative data holder, Sweden), 13 October 2022.

[648] Interview, Arbetsförmedlingen (Beneficiary and administrative data holder, Sweden), 13 October 2022.

- Contact details, number of project participants, number of activities conducted, other descriptive statistics, and data on organisations and project leaders[649].

- Data on project activities, number of participants, and gender balance[650].

Administrative data

- Statistics Sweden: information collected depends on the project. Data include gender, age, country of birth, data from the population register, and level of education. Also, data are collected from the Swedish Public Employment Service on unemployment, and on reduced work capacity due to disabilities, and newcoming immigrants. Information on paid student grants can be obtained from the Swedish Board of Student Finance. In some cases, information on activity compensation and sickness benefit can be obtained from the Swedish Social Insurance Agency[651].

- E.g., employment records to assess effects of projects, including data on background data, employment rate, and transition between studies and work[652].

Collection of participant's data and Consent practises

Arbetsförmedlingen does not use explicit consent as a legal basis for collecting and sharing information about ESF participants. Instead, they use a legal basis based on their legal obligation to carry out ESF projects. Their previous experience with using explicit consent to collect data was that it comes with an administrative burden. Moreover, using explicit consent would not comply with the GDPR because many of the participants are dependent on Arbetsförmedlingen through other contexts for gaining unemployment benefits. Also, a lot of training is not voluntary for unemployed participants as it is connected to unemployment benefits[653].

TSL's data collection is based on consent from participants. Employers share data on employees to a special function at TSL's website or in an Excel file. The Excel file is imported to TSL's system called "Dynamics", which only TSL has access to. This data generates an application that labour unions and employers need to sign. Then, the participants get the information and need to confirm that TSL can process the data, as TSL needs to send the data to the actors that implement the training activities. Employers may share personal data of employees before the employees have given their consent. However, if the employer does not report the personal data of the participants, TSL cannot fully complete their tasks as a beneficiary[654].

Regarding the evaluator interviewed, data used to evaluate ESF are collected through a combination of surveys, interviews, document studies, desk research, literature reviews, and statistical analyses of statistics received from the managing authority and Statistics Sweden. To facilitate collection of data from participants, the evaluator has access to data from the managing authority such as contact details for project participants, organisations, and project leaders. If the evaluator cannot gain access to contact details from the managing

[649] Interview, Trygghetsfonden TSL (Beneficiary, Sweden), 14 October 2022.

[650] Interview, an anonyme consultancy (Evaluator, Sweden), 17 October 2022.

[651] Interview, Statistics Sweden (SCB), 10 October 2022.

[652] Interview, an anonyme consultancy (Evaluator, Sweden), 17 October 2022.

[653] Interview, Arbetsförmedlingen (Beneficiary and administrative data holder, Sweden), 13 October 2022.

[654] Interview, Trygghetsfonden TSL (Beneficiary, Sweden), 14 October 2022.

authority or other organisation, the link to the survey in use is instead sent to project managers who can forward the link to relevant persons. Also, project managers might send contact details upon the evaluator's request that explains the purpose, and after consent from the contact persons. Moreover, other data received from the managing authority has been anonymised, and if the group was too small, it was not possible to access data as it is easier to identify specific persons based on data from a small group[655].

Storing data

The beneficiary Trygghetsfonden stores data on internal servers and in their data system Dynamics. The data must be stored for a period of at least four years according to the managing authority's instructions[656].

The managing authority's instructions[657] specify that project data must be stored until the end of the year four years after receiving the final decision on payment for implementing the ESF project. The period can be extended due to legal proceedings or upon request from the European Commission. The managing authority will then inform about such changes in written form. Data shall be saved in original, attested copies, or on approved data carriers such as a CD, USB, or hard drive.

Data that have been transferred to Statistics Sweden will be stored until the end of the ESF+ programming period[658].

Transferring and accessing data

Transferring participants' personal data

Statistics Sweden is a node for processing personal data about ESF participants. It has a data sharing agreement with the managing authority (the Swedish ESF Council) and Arbetsförmedlingen (Swedish Public Employment Service).

Arbetsförmedlingen said that data shared with SCB is not anonymised at all, as SCB has confidentiality requirements. Arbetsförmedlingen is obliged to share personal data to the ESF Council and SCB, including special categories of personal data, because they are obliged to implement ESF projects. However, to the managing authority, Arbetsförmedlingen can only "show" non-anonymised monitoring samples about project participants[659].

Moreover, TSL shares information with the Swedish ESF Council via a "consolidation report" in an Excel sheet according to a template provided by the Swedish ESF Council. The template includes information on name, social security number, employment status, qualifications achieved, and participation in ESF activities. This information is reported to the Swedish ESF Council every month via SCB according to the same procedures that apply to all ESF beneficiaries. SCB collects all information on behalf of the Swedish ESF

[655] Interview, an anonyme consultancy (Evaluator, Sweden), 17 October 2022.

[656] Interview, Trygghetsfonden TSL (Beneficiary, Sweden), 14 October 2022.

[657] https://www.esf.se/att-driva-projekt/programperiod-2014-2020/projektekonomi/dokumentation-och-arkivering/#S%C3%A5-l%C3%A4nge-ska-ni-spara-projektets-handlingar.

[658] Interview, Statistics Sweden (SCB), 10 October 2022.

[659] Interview, Arbetsförmedlingen (Beneficiary and administrative data holder, Sweden), 13 October 2022.

Council. In addition, TSL will disclose personal data to training providers who have a personal data processing agreement with TSL[660].

Accessing, transferring, and using administrative data

Just as all participant data are reported to SCB, administrative data are accessed through SCB. As described above, SCB accesses administrative data from different public authorities and agencies, including data relevant for ESF monitoring and evaluation. The managing authority said that basically all data comes from SCB.

In practice, the collection of data presupposes that the projects report the participants' personal identity numbers to SCB, which, using this data, collects register data. Depending on the focus of the projects, data can be obtained from registers at SCB, the Swedish Public Employment Service (Arbetsförmedlingen), the Swedish Board of Student Finance (Centrala Studiestödsnämnden) and the Swedish Social Insurance Agency (Försäkringskassan).

According to SCB, the exact information in the Participant Register depends on the project's focus. In addition to personal identity numbers and project data, data on gender, age and country of birth are data from the Population Register and the level of education from the Education Register. To the Participant Register, Statistics Sweden can also link data from the Swedish Public Employment Service on unemployment, reduced work capacity due to disabilities, and newcoming immigrants. Information on paid student grants can be obtained from the Swedish Board of Student Finance. In some cases, information on activity compensation and sickness benefit can be obtained from the Swedish Social Insurance Agency.

According to SCB, the data is used to produce statistics on the results of the ESF projects. After completion of the processing at SCB, all identity data are removed before the material in the form of tables is submitted to the managing authority for further processing and analysis. The results are reported, among other things, to the EU and the Swedish Government.

According to the managing authority's perspective, the managing authority can access data directly from SCB (the data that are useful according to the ESF monitoring and evaluation indicators). Data ordered and received from SCB involves anonymised microdata and 'personal data, mainly for evaluation purposes as it is more useful for that purpose'. However, it is possible for monitoring purposes too. Evaluations are done at several levels: project, programme, and tender evaluations. Personal data and microdata are relevant for counterfactual analyses, to assess effects of ESF support. To facilitate the process of accessing data, the managing authority maintains an ongoing dialogue with SCB via contact persons and communicates the dates on which they need certain data. When ordering additional microdata ad hoc, the length of the process to receive data is usually longer, about two months, as the orders are not according to the normal routines. The length depends on the level of detail in the order and how specific one is on how the data will be used[661].

External evaluators can also order data directly from SCB. These might experience a longer waiting time to receive data from SCB, as the orders are ad hoc. The managing authority usually facilitate the process by endorsing that the external evaluators' orders are on behalf of them[662]. SCB described that de-identified data may be used by researchers and others

[660] Interview, Trygghetsfonden TSL (Beneficiary, Sweden), 14 October 2022.

[661] Interview, The Swedish ESF Council (managing authority), 17 October 2022.

[662] Interview, The Swedish ESF Council (managing authority), 17 October 2022.

who produce statistics. Apart from the ESF managing authority, these can be, e.g., the Swedish Public Employment Service, Swedish Social Insurance Agency, and ESF project evaluators. Such research and statistical activities are subject to statistical confidentiality[663].

The evaluator interviewed confirms such a system. It described that the type of data requested by the evaluator from SCB depends on the projects involved in the assessments, and whether the evaluator's assignment is to assess individual level- or organisation level results. Also, access to data depends on the purpose of using the specific datasets. Most administrative data received from SCB concerned employment records to assess effects of projects, including data on background data, employment rate, and transition between studies and work. In practice, when requesting to buy data from SCB, the evaluator specifies clearly which type of data they want and for what purpose. Then, SCB assesses what data they can deliver, on what level, when, how, and to what cost according to SCB's procedures. Being as specific as possible will facilitate access[664].

Linking data

The process of linking datasets is mostly in the hands of the SCB. To the Participant Register, SCB can link data from, e.g., the Swedish Public Employment Service on unemployment, reduced work capacity due to disabilities, and newcoming migrants[665].

Challenges

Regarding restriction and challenges concerning data processing, there are examples of participants who ask detailed questions about how their personal information is used and shared. Sometime, participants refuse to give consent to the sharing of their personal data. When consent is not given, TSL treats the person as if the person has got a protected identity. As a result, TSL cannot report anything on this person. In such cases, the employer needs to provide information to the actor that implements the training activity. However, this rarely occurs. Moreover, some companies wonder if it is legally correct to share personal data about their employees before the employees have been informed about it or given consent. Sometimes, employers do not want to share the information before getting consent from their employees. If too many participants would deny consent, TSL would not be able to prove that they fulfil their mission[666].

Regarding accessing administrative data, the challenges mentioned by the interviewees concern waiting time and costs involved to access data from SCB[667]. No challenges recorded concerning any specific type of data.

[663] Interview, Statistics Sweden (SCB), 10 October 2022.

[664] Interview, an anonyme consultancy (Evaluator, Sweden), 17 October 2022.

[665] Interview, Statistics Sweden (SCB), 10 October 2022.

[666] Interview, Trygghetsfonden TSL (Beneficiary, Sweden), 14 October 2022.

[667] (1) Interview, The Swedish ESF Council (managing authority), 17 October 2022. (2) Interview, an anonyme consultancy (Evaluator, Sweden), 17 October 2022.

Potential solutions/good practices

Regarding possible improvements, since paying consultancy companies to get legal advice is expensive, it would be better if the Swedish ESF Council could have data protection expertise available to beneficiaries[668].

According to Arbetsförmedlingen, their previous practices regarding collecting explicit consent from the data subjects included administrative challenges. However, these challenges were overcome by changing the legal basis to using a legal basis based on Arbetsformedlingen's legal obligation to carry out ESF projects. The current system is based on their own legal interpretation. However, it would be better if there was a law that stipulates concretely that Arbetsförmedlingen must share data for ESF purposes[669].

Good practice: Arbetsförmedlingen has concluded that they have an obligation to share personal data based on several rules, including

- TVFS 2016:1 – provisions on ESF 2014-2020 from the Swedish Agency for Economic and Regional Growth, on obligations to share information.
- Ordinance (2015:62), § 9 – on state support regarding ESF. It says that a beneficiary is obliged to share information with the Swedish ESF-council to evaluate the ESF, to fulfil Sweden's responsibilities to the European Commission according to Regulation (EU) 651/2014 and Regulation (EU) 1407/2013.
- References in the GDPR to public interest and legal obligations to process personal data.
- Law (2018:259) and Law (2002:546) § 5: 2 regarding data sharing in accordance with law or ordinance.
- The Privacy Law (2009:400), 10 kap. 2 § and 28 § (that stipulates that data sharing can occur for the public authority to fulfil its obligations and if they have a legal obligation to do so).

Guidance/advice

Most interviewees get advice internally and in dialogue with the managing authority. The managing authority has neither sought any advice with the explanation that they do not process non-anonymised administrative data[670].

TSL has received external expertise from consultancy companies on GDPR-related issues but not connected to ESF specifically. This advice has been related to the practice that employers share personal information about their employees before having consent form the employees. The conclusion was that this is legally possible because TSL is obliged to report information on participants that TSL gets fundings for[671].

[668] Interview, Trygghetsfonden TSL (Beneficiary, Sweden), 14 October 2022.

[669] Interview, Arbetsförmedlingen (Beneficiary and administrative data holder, Sweden), 13 October 2022.

[670] Interview, The Swedish ESF Council (managing authority), 17 October 2022.

[671] Interview, Trygghetsfonden TSL (Beneficiary, Sweden), 14 October 2022.

8.4. Annex IV – Focus Group summary

Final minutes – Focus Group

Smart ways to monitor the ESF: how to gain access to administrative data while complying with data protection rules

Specific Contract No VC/2022/0148 under the Framework Contract No VC/2021/0337

Thursday 16 March 2023 – 14:00-16:30

Microsoft Teams

Workshop organisers

Milieu	**Fondazione Giacomo Brodolini**	**European Commission**

Workshop participants

Country	Stakeholder type	Organisation
AT	Managing authority	Federal Ministry for Employment and Economy
BG	Managing authority	Ministry of Labour and Social Policy, MA of Human Resources Development Programme 2021-2027
DE	Managing authority	Federal Ministry for Employment and Social Affairs
EE	Managing authority	Ministry of Finance, coordinating Structural Fund evaluations
EE	Managing authority	Ministry of Social Affairs
ES	Managing authority	Administrative Unit of the European Social Fund
ES	Managing authority	Administrative Unit of the European Social Fund
ES	Evaluator	Red2Red (Spanish Consultancy specialised in ESIF Funds evaluation)
ES	Evaluator	Red2Red (Spanish Consultancy specialised in ESIF Funds evaluation)
ES	Evaluator	Red2Red (Spanish Consultancy specialised in ESIF Funds evaluation)
ES	Evaluator	Red2Red (Spanish Consultancy specialised in ESIF Funds evaluation)
HU	Managing authority	Ministry of Regional Development
IE	Managing authority	PEIL

Country	Stakeholder type	Organisation
IE	Managing authority	PEIL
IE	Managing authority	PEIL
IE	Managing authority	PEIL
IE	Intermediary Body	Department of Social Protection
IE	Intermediary Body	Department of Social Protection
IE	Intermediary Body	Department of Social Protection
IE	Intermediary Body	Department of Social Protection
IE	Intermediary Body	Department of Social Protection
IE	Intermediary Body	Department of Social Protection
IT	Managing authority	Territorial Cohesion Agency
LV	Managing authority	Division of Evaluation Unit of EU Funds Strategy Department, Ministry of Finance
NL	Managing authority	Ministry of Social Affairs and Employment, Managing authority for ESF+ and Just Transition Fund (data collection and transmission)
PL	Managing authority	Ministry of Development Funds and Regional Policy
RO	Managing authority	National Unemployment Agency
SE	Managing authority	The Swedish ESF Council

Number of organisations, countries, and stakeholder types represented in the workshop

Organisations	Countries	Stakeholder types
16	13	3

Introduction and background

To ensure the formulation of robust and practical solutions that combine the monitoring and evaluation needs of the ESF/ESF+ with the fundamental right to data protection, the aim of the focus group was to assess the main issues at stake and to jointly explore possible solutions. The discussion held will support the development of the final recommendations proposed in the study "Smart ways to monitor and evaluate the ESF: how to gain access to administrative data while complying with data protection rules".

To support the discussion, a background paper was circulated to the invited participants prior to the meeting, explaining the purpose of the study and the focus group, the focus group methodology, and a number of issues and solutions that had been identified so far in the study.

The issues and solutions discussed were based on the results of desk research and interviews with key stakeholders in nine EU Member States (i.e., Austria, Germany, Spain, France, Ireland, Italy, Poland, Romania, and Sweden), combined with a more in-depth legal analysis focusing on three EU Member States (i.e., Austria, Spain and Romania). Participants were invited to:

- provide feedback on the proposed issues at stake; and
- discuss possible solutions according to a set of criteria, i.e., relevance, political feasibility, legal feasibility, and administrative feasibility.

The proposed solutions were grouped into three main themes:

- Understanding and complying with data protection law
- Overcoming national particularities
- Organisational issues affecting effective access to administrative data.

Under each theme, the focus group organisers described a number of challenges (issues) and solutions that respond to these challenges as indicated below in these minutes.

To facilitate the discussion, participants could first vote on the relevance of each sub-solution and then discuss the feasibility of implementing the relevant solutions. Participants could also suggest new solutions and develop why certain solutions are relevant or not, and why certain solutions are feasible or not.

Theme 1 – Understanding and compliance with data protection law: Providing guidance at national level to avoid ambiguity in interpreting the chosen legal basis.

Providing guidance at national level to avoid ambiguity in interpreting the chosen legal basis

ISSUE 1

Several options among legal bases to use and diverging interpretations of EU and national laws about the most appropriate legal basis for accessing administrative data for ESF/ESF+ monitoring and evaluation purposes.

SOLUTION 1

1.a) Encourage the Member States to consult their national Data Protection Authority (DPA) on the choice of the legal basis.

1.b) Exploring possibilities to use legal bases such as ‘public interest’ or ‘legal obligation’ instead of (explicit) consent for accessing administrative data.

Results of the vote regarding the relevance of each solution:

Solutions	Number of votes	Stakeholders
Encourage the Member State to consult their national Data Protection Authority (DPA) on the choice of the legal basis	43 % (6 votes)	• DE, Federal Ministry for Employment and Social Affairs (MA) • BG, Ministry of Labour and Social Policy (MA) • ES, Administrative Unit of the European Social Fund (MA) • NL, Ministry of Social Affairs and Employment (MA) • RO, National Unemployment Agency (MA) • IE, Department of Social Protection (Intermediary Body)
Exploring possibilities to use legal bases such as 'public interest' or 'legal obligation' instead of (explicit) consent for accessing administrative data	57 % (8 votes)	• HU, Ministry of Regional Development (MA) • BG, Ministry of Labour and Social Policy (MA) • NL, Ministry of Social Affairs and Employment (MA) • PL, Ministry of Development Funds and Regional Policy (MA) • LV, Ministry of Finance (MA) • IE, PEIL (MA) • AT, Federal Ministry for Employment and Economy (MA) • ES, Spanish Consultancy specialised in ESIF Funds evaluation
Total of votes	**14 votes**	

Discussion on the feasibility of implementing the relevant solutions:

- **Representative from BG, Ministry of Labour and Social Policy (managing authority):** We use both these solutions. We use data from another institution and we also consulted our Data Protection Authority (DPA) in Bulgaria.

- **Milieu**: BG was not one of the 9 Member States covered in this study. Have you already considered changes to the legal framework in BG or do you consider that these 'soft solutions' are sufficient? Can you base access to administrative data on the two legal bases proposed on the basis of the existing legal framework?

- **Representative from BG, Ministry of Labour and Social Policy (managing authority):** They are provided for in the Bulgarian Data Protection Act, which is based on the GDPR. We do not need to change our legislation at this stage.

- **Representative from IE, Department of Social Protection (Intermediary Body)**: Comment on solution 1.a): We have a Data Protection Officer within the Ministry with whom we would discuss these types of issues in the first instance. We would not contact our national DPA on such matters unless there was a comprehensive issue.

- **Milieu**: A good suggestion for organisations with such internal departments is to look within that department first for advice.

- **Representative from HU, Ministry of Regional Development (managing authority)**: Encouraging Member States to consult the DPA means passing the problem on to the Member States. Could it not be said that there is a central obligation from the Commission for us to collect data for monitoring and evaluation? Why do we have to find an explanation for why we have to share the data when the reason is that we have to?

- ***Comment in the chat from a representative from AT, Federal Ministry for Employment and Economy (managing authority)****: A centralised solution would be very helpful!*

- **Milieu**: We understand that this is something that stakeholders would appreciate and we are trying to explore this further. It is not easy to understand who we could turn to at EU level for such horizontal advice (the EDPB - which would not normally deal with such specific issues, and the European Data Protection Supervisor - who is more competent for the processing of personal data by the institutions). In preparing this study, we looked at their opinions and guidance on the interpretation of the GDPR, which may provide some solutions.

- What about explicit consent as a legal basis? We have seen a shift from consent to the legal obligation and public interest as legal bases (especially in IE and SE).

- **Representative from RO, National Unemployment Agency (managing authority)**: This issue was discussed with the RO DPA last year. The idea to use public interest or legal obligation as legal bases was rejected because there is no explicit paragraph that mentions it. The RO DPA asks us not to use a legal obligation as a legal basis because the important element is the protection of personal data. I agree with their position, but we still have problems with the transmission of personal data.

- ***Comment in the chat from a representative from LV, Ministry of Finance (managing authority)****: The managing authority needs a very explicit obligation written into the regulation to collect micro-level data from participants.*

Enabling reuse of administrative data and further processing for scientific research

ISSUE 2

Reuse of data from existing administrative datasets is not always possible due to ambiguity in the choice of legal basis and further processing of such data is disabled due to not considering evaluations as scientific research.

SOLUTION 2

2.a) Establish a clearer legal basis for the reuse of administrative data at national level.

2.b) Conclude data sharing agreements to facilitate the exchange of administrative data for ESF+ purposes.

2.c) National DPAs to provide opinions/guidelines on the compatible purposes and on the possibility to rely on scientific research for further processing of personal data as well as its impact on data subjects' rights.

Results of the vote regarding the relevance of each solution:

Solutions	Number of votes	Stakeholders
Establish a clearer legal basis for the reuse of administrative data at the national level	25 % (4 votes)	• HU, Ministry of Regional Development (MA) • LV, Ministry of Finance (MA) • IE, PEIL (MA) • RO, National Unemployment Agency (MA)
Conclude data sharing agreements to facilitate the exchange of administrative data for ESF+ purposes	44 % (7 votes)	• ES, Spanish Consultancy specialised in ESIF Funds evaluation • BG, Ministry of Labour and Social Policy (MA) • NL, Ministry of Social Affairs and Employment (MA) • LV, Ministry of Finance (MA) • IE, PEIL (MA) • AT, Federal Ministry for Employment and Economy (MA) • ES, Administrative Unit of the European Social Fund (MA)
National DPAs to provide opinions/guidelines on the compatible purposes and on the possibility to rely on scientific research for further processing of	31 % (5 votes)	• BG, Ministry of Labour and Social Policy (MA) • HU, Ministry of Regional Development (MA)

Solutions	Number of votes	Stakeholders
personal data as well as its impact on data subjects' rights		• IE, Department of Social Protection (Intermediary Body) • RO, National Unemployment Agency (MA) • DE, Federal Ministry for Employment and Social Affairs (MA)
Total of votes	**16 votes**	

Discussion on the feasibility of implementing the relevant solutions:

- ***Comment in the chat from a representative from AT, Federal Ministry for Employment and Economy (managing authority)***: *The definition of "scientific research" is based on EU law. Will there be a central clarification?*
- **Milieu**: Explained what the term means. The European Data Protection Supervisor is working on guidelines on this issue. At the moment, there is a preliminary opinion from the European Data Protection Supervisor, which interprets scientific research quite narrowly. It would also depend on national laws, which supplement the GDPR, and other guidelines issued by the DPA.
- ***Comment in the chat from a representative from LV, Ministry of Finance (managing authority)****: Yes, DPAs are incredibly creative in interpretations about data protection.*
- **Representative from AT, Federal Ministry for Employment and Economy (managing authority)**: In AT, the DPA has been very restrictive, so unless there is any guideline at EU level that can be interpreted more broadly, it will be interpreted as narrowly as possible. Anything that is given on a central basis would be really helpful. We tried to look at the legal basis for scientific research some time ago, but there was no way to define it and to conduct evaluations as scientific research. Our main challenge is the regulation as such - it will always be interpreted more strictly. For example, when we tried to contact people after parental leave, we were not allowed to because we had not asked them if they wanted to be contacted.
- ***Comment in the chat by a representative from DE, Federal Ministry for Employment and Social Affairs (managing authority)****: I agree with the [AT, Federal Ministry for Employment and Economy (managing authority)] comment.*
- **Representative from LV, Ministry of Finance (managing authority):** I also agree that they manage to find an interpretation that is so narrow that it is not possible to get any data at all, because it is not explicitly written that you are allowed to collect it.
- **Representative from DE, Federal Ministry for Employment and Social Affairs (managing authority)**: They underlined what the two previous speakers said, that it is quite difficult to work with the DPA because they have a very restrictive interpretation of the GDPR. It would be very helpful if there could be more clarification from the EU on the GDPR and its wording.
- **Milieu**: Asked about expanding further the discussion on data sharing agreements.

- **Representative from IE, PEIL (managing authority)**: We do not really use the term data sharing agreement, but the managing authority would have administrative agreements with the different beneficiaries and intermediary bodies. Certain bodies would have data sharing agreements with bodies at a lower administrative level. We also have separately a number of data protection agreements, which are more related to GDPR compliance. On another point, and in line with what AT, DE and LV said, the DPO in IE has a very strict interpretation of the GDPR requirements, so it is not beneficial to ask for their advice. I suppose we would use previous templates that would be in the system. We have administrative arrangements that cover everything - data sharing would be a small part.
- **Representative from LV, Ministry of Finance (managing authority):** There should be some sort of solution to the problems we face in LV. Is it possible to somehow write down the rules of how to store this administrative data? It is a huge amount of work to collect them and delete them after the research is done. We are looking for a solution to store it for the next ex-post evaluation, so that we do not have to go back to the agencies and ask them again to retrieve this data. This is not our number 1 problem, but it would be useful to think about it.
- **Milieu:** From a data protection perspective, it is difficult to foresee that the data will still be accurate in five years and to have the legal basis to keep it for that long with a compatible purpose. Data sharing agreements could better explain these rules (how long certain data can be used, storage, collection, retention, purpose of use, etc.).

Minimising processing of special categories of personal data

ISSUE 3

Processing special categories of personal data is not always possible.

SOLUTION 3

3.a) Use alternative methods to process special categories of personal data (e.g., informed estimates).

3.b) When processing special categories of personal data, apply the principle of data minimisation and ensure an appropriate level of security (for instance using pseudonymisation and concluding a DPIA).

3.c) Consider national rules on legal basis and on lifting the ban on processing special categories of personal data and seek advice of data protection experts (national DPAs, Data Protection Officers (DPOs), or consultants).

Results of the vote regarding the relevance of each solution:

Solutions	Number of votes	Stakeholders
Use alternative methods to process special categories of personal data (e.g., informed estimates)	7 % (1 vote)	• AT, Federal Ministry for Employment and Economy (MA)
When processing special categories of personal data, apply the principle of data minimisation and ensure an appropriate level of security (for instance through the use of pseudonymisation and conclusion of a DPIA)	69 % (9 votes)	• ES, Administrative Unit of the European Social Fund (MA) • DE, Federal Ministry for Employment and Social Affairs (MA) • BG, Ministry of Labour and Social Policy (MA) • NL, Ministry of Social Affairs and Employment (MA) • ES, Spanish Consultancy specialised in ESIF Funds evaluation • IE, PEIL (MA) • IE, Department of Social Protection (Intermediary Body) • AT, Federal Ministry for Employment and Economy (MA) • RO, National Unemployment Agency (MA)
Consider national rules on legal basis and on lifting the ban on processing special categories of personal data and seek advice of data protection experts (national DPAs, Data Protection Officers (DPOs), or consultants)	23 % (3 votes)	• BG, Ministry of Labour and Social Policy (MA) • IE, PEIL (MA) • LV, Ministry of Finance (MA)
Total of votes	**13 votes**	

Discussion on the feasibility of implementing the relevant solutions:

- **Comment in the chat from a representative from AT, Federal Ministry for Employment and Economy (managing authority)**: For Austria: 3.c) would not be possible – as again it results from the GDPR. No national law could change the regulation.

- **Representative from AT, Federal Ministry for Employment and Economy (managing authority):** We have used pseudonymisation quite a lot, but it does not really solve the first problem of finding people in the registers to get an identifier to access the data. Thus, data minimisation/pseudonymisation is not helpful for accessing personal data. On 3.c), I do not see how we could change the regulation through national law, so I do not really understand solution c).

- **Milieu:** When processing special categories of personal data, you need to secure a legal basis (Article 6 GDPR) and find one of the options to lift the prohibition on processing special categories of personal data. These are usually further analysed under national law. Therefore, there may be some national specificities or a bit more leeway when processing data for scientific research, for example.

- Could you explain the good practice of pseudonymising data, to understand how it can facilitate the processing of data?

- **Representative from AT, Federal Ministry for Employment and Economy (managing authority):** Our statistical unit does it quite regularly. We have separate contracts. We have a contract with an institute. As soon as we have data from the social security situation, for example, it is transmitted to this institute, which pseudonymises it, and then this list (pseudonymised) is given to the evaluators. It works very well, but there needs to be a separate contract for that part to ensure data protection.

- **Costanza Pagnini:** Question for Martina: You say that pseudonymising data can be a solution, but at the same time it does not allow you to link individual data. Then the scope of the evaluation and the effectiveness is somewhat limited, because you can say something about the group, but you cannot link the stories of different individuals to other administrative records, for example.

- **Representative from AT, Federal Ministry for Employment and Economy (managing authority):** Actually, you can. Once it is pseudonymised, you can use this number to access the registers. But now we have problems getting access to the personalised information. We are not allowed to use the identifier to find people in the social security system, for example. We need a separate and unique identifier, which we do not have for the ESF.

- **Milieu**: Explained the difference between anonymisation and pseudonymisation. Pseudonymisation would still be personal data because you can link it back to an individual. If you have certain data points at the end, you might be able to link back to the identifier and the name.

- **Representative from AT, Federal Ministry for Employment and Economy (managing authority): T**here are several different identifiers, and you are only allowed to use identifiers for your purpose. In AT, we have two identifiers for labour market measures, but these are only used by the public employment service, and the ESF is not administered by the public employment service, so we do not have these identifiers. We can no longer use the social security number because it can only be used for health measures. We know what to do once we have an identifier and we work with pseudonymisation and it works very well but at the moment we lack the identifier.

Theme 2: Overcoming national particularities – Enhancing the awareness of national-level rules covering the processing of administrative data

Enhancing the awareness of national-level rules covering the processing of administrative data

ISSUE 4

Lack of understanding and/or awareness of national legal frameworks for the processing of administrative data

SOLUTION 4

4.a) Consider national rules in conjunction with EU law and seek advice, guidance, and/or participate in trainings of data protection experts (national DPAs, DPOs, or consultants).

4.b) Perform data protection impact assessments (DPIAs) for new projects and encourage sharing promising examples or templates of such assessments.

Results of the vote regarding the relevance of each solution:

Solutions	Number of votes	Stakeholders
Consider national rules in conjunction with EU law and seek advice, guidance, and/or participate in trainings of data protection experts (national DPAs, DPOs, or consultants)	66 % (6 votes)	• ES, Spanish Consultancy specialised in ESIF Funds evaluation • IE, PEIL (MA) • NL, Ministry of Social Affairs and Employment (MA) • BG, Ministry of Labour and Social Policy (MA) • LV, Ministry of Finance (MA) • AT, Federal Ministry for Employment and Economy (MA)
Perform data protection impact assessments (DPIAs) for new projects and encourage sharing promising examples or templates of such assessments	33 % (3 votes)	• NL, Ministry of Social Affairs and Employment (MA) • IE, Department of Social Protection (Intermediary Body) • LV, Ministry of Finance (MA)
Total of votes	**9 votes**	

Discussion on the feasibility of implementing the relevant solutions:

- **Milieu:** Milieu gave some background on these issues. It seems that in some Member States there would be additional barriers to access to data (additional provisions or national implementation), for example in AT the processing of ethnicity was not allowed, and in RO you need a clear basis in the law, meaning that a data sharing agreement would not be sufficient for allowing the transmission of data

between two public authorities. This is why we suggested to look more closely at national data protection rules, as EU rules may not be sufficient.

- **Representative from LV, Ministry of Finance (managing authority):** Additional training is needed for us as managing authorities or project implementation, but also for data protection specialists as well, because they almost always rely on what is explicitly written in normative acts. There is no plasticity in the implementation. For example, last year we needed micro-level participant's data, we almost got an agreement with the agency that collects data, but then data protection specialists said that they could not give the data. After some time, we managed to convince them that this data is needed for ex-post evaluation and that the aim is legal. There are also instances of good cooperation.

- **Representative from AT, Federal Ministry for Employment and Economy (managing authority):** We only carry out data protection impact assessments (DPIA) when we see the possibility of a significant impact on individual rights. We have never done a DPIA for the ESF. We do not see the need to do a DPIA at all, because it would mean that we see a major risk in the use of ESF data, which we do not see. I am not sure what the benefit would be.

- **Milieu:** Some organisations do it regularly as a good practice to prepare for all possible risk scenarios before starting to process data. DPIA introduces some kind of safeguards such as pseudonymisation, seeing if the legal basis is a bit weak, etc. It can be used as a privacy tool to make sure that everything is covered.

- **Representative from DE, Federal Ministry for Employment and Social Affairs (managing authority)**: I agree with AT, which is why I did not choose 4.b). I think it is a very good idea to share promising ideas with other Member States, but I hesitated because we do not really use DPIAs in the context of ESF.

Promoting the exchange of good practices

ISSUE 5

Lack of mutual learning between Member States regarding data protection-related issues concerning access to administrative data for ESF/ESF+ purposes

SOLUTION 5

5.a) Promote the exchange of good practices between Member States on access to administrative data for ESF/ESF+ purposes.

5.b) Continue to organise contact points where relevant stakeholders from Member States can meet and network.

5.c) Promotion of the development of a practical document and/or handbook for Member States and/or competent authorities.

Results of the vote regarding the relevance of each solution:

Solutions	Number of votes	Stakeholders
Promote the exchange of good practices between Member States on access to administrative data for ESF/ESF+ purposes	33 % (7 votes)	• IE, PEIL (MA) • NL, Ministry of Social Affairs and Employment (MA) • LV, Ministry of Finance (MA) • AT, Federal Ministry for Employment and Economy (MA) • BG, Ministry of Labour and Social Policy (MA) • DE, Federal Ministry for Employment and Social Affairs (MA) • ES, Administrative Unit of the European Social Fund (MA)
Continue to organise contact points where relevant stakeholders from Member States can meet and network	19 % (4 votes)	• IE, PEIL (MA) • NL, Ministry of Social Affairs and Employment (MA) • BG, Ministry of Labour and Social Policy (MA) • DE, Federal Ministry for Employment and Social Affairs (MA) • IE, Department of Social Protection (Intermediary Body) • LV, Ministry of Finance (MA)
Promotion of the development of a practical document and/or handbook for Member States and/or competent authorities	48 % (10 votes)	• IE, PEIL (MA) • NL, Ministry of Social Affairs and Employment (MA) • HU, Ministry of Regional Development (MA) • RO, National Unemployment Agency (MA)LV, Ministry of Finance (MA) • AT, Federal Ministry for Employment and Economy (MA) • BG, Ministry of Labour and Social Policy (MA) • DE, Federal Ministry for Employment and Social Affairs (MA) • ES, Spanish Consultancy specialised in ESIF Funds evaluation • IE, Department of Social Protection (Intermediary Body)
Total of votes	**21 votes**	

Discussion on the feasibility of implementing the relevant solutions:

- **Representative from HU, Ministry of Regional Development (anaging authority):** If I understand correctly, option b) is something like this workshop. It is fruitful and very good to discuss these issues in person. But the good solution would be to have something that everyone can reach and read. Thus, option b) is good, but I think option c) is better.

- **Representative from DE, Federal Ministry for Employment and Social Affairs (managing authority):** Suggestion: It seems to me that the DPAs are in a very strong position and sometimes very restrictive. As we are now discussing how an exchange could work, I would encourage the European Commission to involve the DPAs in this discussion.

Theme 3: Organisational issues affecting effective access to administrative data -Centralising data processing

ISSUE 6
Low level of interoperability of the national registers of administrative data and difficulties to access these due to decentralised data processing.

SOLUTION 6

6.a) Initiatives to centralise data processing, including the hosting of data.

6.b) Use pseudonymisation

6.c) Promote the centralisation of the management and coordination of access to administrative data for the purposes of ESF+ monitoring and evaluation.

Centralising data processing

Results of the vote regarding the relevance of each solution:

Solutions	Number of votes	Stakeholders
Initiatives to centralised data processing, including the hosting of data	30 % (3 votes)	• IE, PEIL (MA) • BG, Ministry of Labour and Social Policy (MA) • RO, National Unemployment Agency (MA)
Encourage the use of pseudonymisation	30 % (3 votes)	• IE, Department of Social Protection (Intermediary Body) • BG, Ministry of Labour and Social Policy (MA) • AT, Federal Ministry for Employment and Economy (MA)
Promote the centralisation of the management and coordination of access to administrative data for the purposes of ESF+ monitoring and evaluation	40 % (4 votes)	• IE, PEIL (MA) • ES, Spanish Consultancy specialised in ESIF Funds evaluation • LV, Ministry of Finance (MA) • AT, Federal Ministry for Employment and Economy (MA)
Total of votes	**10 votes**	

Discussion on the feasibility of implementing the relevant solutions:

- **Representative from LV, Ministry of Finance (managing authority)**: All options are fine. But from what I have heard from DE and AT, this institutional level is quite different from country to country, and it might be easier to use one institution. For us it is easier to use an already established system (in this case the Cohesion Policy monitoring systems that collect all the data from projects). It is easier to choose c) because we can develop services with agencies that contain some more information. The system can be used systematically and automatised. It is also easier to have all the data in one place and to give all the data to the evaluators already anonymised. Pseudonymisation is difficult to use because you would need an institute to recombine all the data. The chain is too long and sometimes it can be very expensive.

- **Representative from BG, Ministry of Labour and Social Policy (managing authority):** We are trying to centralise our database. It will not be managed by the National Statistical Institute, although they will help, but by the Council of Ministers, which is responsible for the whole database of all EU funds. In BG, it is difficult to have all the registers in one place, because the different institutions do not allow access to personal data, so we have agreements with specific institutions. In order not to lose personal data (as a ministry we are administrator of personal data), we send them the file with all the data we have, they complete the data, send the file back to us, clean the data, and then transmit it to the evaluator. Therefore, the evaluator cannot identify the individuals. That is how we solve the problem of working with different institutions. We still do not have a single database, and we do not know when we will have one, but it is under discussion. For evaluation purposes, we use pseudonymisation. We hope that one day we will have centralised data system, but that will be in the future. The problem is not the GDPR but the fact that the institutions do not really agree to link the data.

- **Milieu**: Are these agreements on a general level or specifically for ESF?

- **Representative from BG, Ministry of Labour and Social Policy (managing authority):** The first decision was that the agreement between the ministries and the National Social Security Institute should cover not only the needs of the ESF and the managing authorities, but also those of the other policy-making departments. But it did not work. Our agreement at this point is only for our monitoring and evaluation purposes/ESF managing authorities.

- The funding bodies and our institution are administrative data holders. Therefore, we can reuse personal data. However, we are not allowed to transmit personal data to external evaluators, so we clean it and then we give it to them.

- **Milieu in the chat**: *If I understand you correctly, you have agreements with national authorities under which you can transmit personal data. You then anonymise the data and transmit it to the evaluators?*

- **Representative from BG, Ministry of Labour and Social Policy (managing authority) in the chat**: *yes, exactly - in the agreement it is stated the data will be pseudonymised and after this data will be provided to the evaluation team for conducting evaluation*.

Planning data access well in advance to avoid unnecessary costs and delays

ISSUE 7

Financial and human resource costs of requesting, purchasing or accessing administrative data

SOLUTION 7

7.a) Plan well in advance what administrative data will be needed to complement or replace direct data collection for ESF+ monitoring and evaluation.

7.b) Managing authorities to coordinate planning with administrative data holders who may know what data is available.

7.c) Plan the scope of the data needed to avoid rejections based on a population sample that is too small.

Results of the vote regarding the relevance of each solution:

Solutions	Number of votes	Stakeholders
Plan well in advance what administrative data will be needed to complement or replace direct data collection for ESF+ monitoring and evaluation	33 % (5 votes)	• IE, PEIL (MA) • ES, Spanish Consultancy specialised in ESIF Funds evaluation • RO, National Unemployment Agency (MA) • AT, Federal Ministry for Employment and Economy (MA) • BG, Ministry of Labour and Social Policy (MA)
Managing authorities to coordinate planning with administrative data holders who may know what data is available	53 % (8 votes)	• IE, PEIL (MA) • ES, Spanish Consultancy specialised in ESIF Funds evaluation • LV, Ministry of Finance (MA) • RO, National Unemployment Agency (MA) • IE, Department of Social Protection (Intermediary Body) • AT, Federal Ministry for Employment and Economy (MA) • ES, Administrative Unit of the European Social Fund (MA) • BG, Ministry of Labour and Social Policy (MA)
Plan the scope of the data needed to avoid rejections based on a population sample that is too small	13 % (2 votes)	• IE, PEIL (MA)

Solutions	Number of votes	Stakeholders
		• BG, Ministry of Labour and Social Policy (MA)
Total of votes	**15 votes**	

Discussion on the feasibility of implementing the relevant solutions:

- **Representative from AT, Federal Ministry for Employment and Economy (managing authority):** Difference between monitoring and evaluation, what you have to collect for monitoring is clearer and easy to plan. It is very difficult to plan for evaluation, it really depends on the individual set of evaluations, and you cannot really plan in advance for such a period. For each new individual evaluation, it is a new and step-by-step process. We had the chance to have evaluators already contracted, so there was no issue. Evaluators were involved in the whole process of defining the data before the evaluation. We need several steps to clarify which data they will need, which period will be covered, you need to have a deep insight, knowledge on the evaluation side, not only on the managing/practical side. To have access to the data, you need to know exactly which data you will need, and for that, you need to be deep in the planning of the evaluation. One challenge is that you cannot ask external evaluators about these issues in this planning process because they would then be excluded from the tender.

- Another aspect is the definition of the data, which is very different. We have tried to use more registers and not collect so much data from individuals, and in the end, we found that we will stick to collecting data from individuals because the definitions are not what the ESF requires. Everybody is using their own definition and adapting the definition. This reduces the usability of the data.

- **Representative from LV, Ministry of Finance (managing authority)**: I absolutely agree with the previous speaker. Monitoring data is easy to collect because it is mandatory, but it is not the same for evaluations. The most important thing for us now is to understand what kind of data institutions have. In the last planning period, we also identified several databases that are already quite inconsistent internally; not very clean for evaluation purposes. We would like to know which institution will have this data before we do anything about evaluation. In these procurement processes, we cannot ask bidders to do all the work and what kind of data they will need until they have won the competition.

Last words from the European Commission

The European Commission concluded the meeting by saying that the discussion had been very interesting and rich. This is a complex issue, and we need to take it forward. The European Commission, therefore, thanked everyone for all the input, the discussions and for bringing up many issues. Solutions need to be combined and there is still a lot to do and many more ideas to consider. All in all, it was very interesting and enlightening.

Summary and conclusions

Focus group participants had the opportunity to vote on the relevance - and discuss the feasibility - of a total of 19 proposed solutions. The most relevant solutions (with over five votes) were, according to the participants:

- Encourage the Member States to consult their national DPA on the choice of the legal basis.
- Explore possibilities to use legal bases such as ‘public interest’ or ‘legal obligation’ instead of (explicit) consent for accessing administrative data.
- Conclude data sharing agreements to facilitate the exchange of administrative data for ESF+ purposes.
- When processing special categories of personal data, apply the principle of data minimisation and ensure an appropriate level of security.
- Consider national rules in conjunction with EU law and seek advice, guidance, and/or participate in training of data protection experts.
- Promote the exchange of good practices between Member States on access to administrative data for ESF/ESF+ purposes.
- Promotion of the development of a practical document and/or handbook for Member States and/or competent authorities.
- Managing authorities to coordinate planning with administrative data holders who may know what data is available.

Some of the key takeaways from the discussion were:

- The need for obligations at national or EU level to facilitate data collection.
- That the legal interpretations of national DPAs can be very restrictive, which can be a barrier to asking for their guidance.
- The need for guidelines and a definition of scientific research at EU level.
- Centralising the management and coordination of access to administrative data can be a relevant solution because it is easier to have all the data in one place and to give all the data to the evaluators already anonymised (according to one participant).
- It can be difficult to plan evaluation processes because it takes several steps to clarify in detail which data are needed and from which period.
- Data may be defined differently by different data holders, which can reduce the usability of data from administrative registers.

A summary for each topic of the Focus Group is included below.

Providing guidance at national level to avoid ambiguity in interpreting the chosen legal basis

Both sub-solutions were assessed as rather equally relevant to the participants. Regarding solution 6.a, an Irish intermediary body developed that they would need to consult their national DPA only if there would be a major issue, since internal DPOs are normally sufficient to consult.

Regarding solution 1.b, three participants mentioned that an obligation to collect data for ESF monitoring and evaluation would facilitate data collection. managing authorities from HU and AT called for a central EU-level obligation, while a Latvian managing authority explained that they need an explicit obligation written in national law.

Solution	Votes (relevance)
1.a) Encourage the Member States to consult their national DPA on the choice of the legal basis.	6
1.b) Exploring possibilities to use legal bases such as 'public interest' or 'legal obligation' instead of (explicit) consent for accessing administrative data. (8 votes)	8

Enabling reuse of administrative data and further processing for scientific research

2.b was considered by participants to be the most relevant solution. The discussion on this solution was limited, but the Irish managing authority explained that although the term data sharing agreement is not used, the managing authority has several data processing agreements with beneficiaries and intermediaries.

However, several participants stated that the legal interpretations of national DPAs are very restrictive. For example, the Latvian managing authority explained that such narrow interpretations exclude almost all data collection. In addition, the Irish managing authority did not find it very useful to ask their DPA for advice because of these strict interpretations.

Managing authorities from AT and DE called for clarifications at EU level to facilitate data collection. According to the Austrian managing authority, there is a need for guidelines and a definition of scientific research at EU level. Currently, evaluations are not considered as scientific research in AT.

Solution	Votes (relevance)
2.a) Establish a clearer legal bases for the reuse of administrative data at the national level.	4
2.b) Conclude data sharing agreements to facilitate the exchange of administrative data for ESF+ purposes. (7 votes)	7
2.c) National DPAs to provide opinions/guidelines on the compatible purposes and on the possibility to rely on scientific research for further processing of personal data as well as its impact on data subjects' rights.	5

Minimising processing of special categories of personal data

3.b was the most relevant solution according to the participants. The Austrian managing authority explained that pseudonymisation is often used in AT. For this purpose, the managing authority commissions an institute to pseudonymise the data, which are then transmitted to an evaluator. It is technically possible to use pseudonymised data to link individual data using unique identifiers. However, this is not currently possible because there is no unique identifier for ESF, and the managing authority is not allowed to use an identifier such as the social security number to identify individuals in the social security system. Therefore, according to the managing authority, pseudonymisation does not facilitate access to personal data in Austria.

Concerning 3(c), the Austrian managing authority did not find the solution relevant, as it found it difficult to see how national legislation could be changed or facilitate the processing of special categories of personal data.

Solution	Votes (relevance)
3.a) Use alternative methods to process special categories of personal data (e.g., informed estimates).	1
3.b) When processing special categories of personal data, apply the principle of data minimisation and ensure an appropriate level of security (for instance using pseudonymisation and concluding a DPIA).	9
3.c) Consider national rules on legal basis and on lifting the ban on processing special categories of personal data and seek advice of data protection experts (national DPAs, Data Protection Officers (DPOs), or consultants).	3

Enhancing the awareness of national-level rules covering the processing of administrative data

4.a was considered the most relevant solution by the participants. The Latvian managing authority developed its answer by saying that DP specialists also need training, as it had happened that a DP specialist in an agency refused them access to micro-level personal data. The managing authority later convinced the agency that access was possible because of the legal requirements.

4.b was considered less relevant as according to the managing authorities in AT and DE, DPIAs are not used in the ESF context. The German managing authority argued that there are no major risks related to processing of the ESF data.

Solution	Votes (relevance)
4.a) Consider national rules in conjunction with EU law and seek advice, guidance, and/or participate in trainings of data protection experts (national DPAs, DPOs, or consultants).	6
4.b) Perform data protection impact assessments (DPIAs) for new projects and encourage sharing promising examples or templates of such assessments.	3

Promoting the exchange of good practices

5c was the most relevant solution for the participants. According to the Hungarian managing authority, published documents accessible to all would be the most inclusive medium to promote good practice.

Concerning solution 5(b), the German managing authority suggested involving DPAs in such discussion fora, as they usually interpret data protection legislation in a restrictive way.

Solution	Votes (relevance)
5.a) Promote the exchange of good practices between Member States on access to administrative data for ESF/ESF+ purposes.	7
5.b) Continue to organise contact points where relevant stakeholders from Member States can meet and network.	4
5.c) Promotion of the development of a practical document and/or handbook for Member States and/or competent authorities.	10

Centralising data processing

6.c was the most relevant solution for participants, although not significantly more relevant than the other two solutions. For the Latvian managing authority, 6.c is the best solution because it is easier to have all the data in one place and to give all the data to the evaluators, already anonymised. Such a system could also be used more systematically and automatically.

Regarding solution 6.b, the Latvian managing authority argued that pseudonymisation is difficult to use because you need an institute to recombine all the data. Also, because it can be complex and expensive.

Concerning solution 6.a, the Bulgarian managing authority explained that they are currently trying to centralise their ESF funds database to be hosted by the Council of Ministers. However, it is very difficult to centralise all registers in one place as different institutions may not allow access to personal data. In practice, the Bulgarian managing authority uses a third party to process and clean the data for transmission to the evaluators in an anonymised form.

Solution	Votes (relevance)
6.a) Initiatives to centralise data processing, including the hosting of data.	3
6.b) Use pseudonymisation	3
6.c) Promote the centralisation of the management and coordination of access to administrative data for the purposes of ESF+ monitoring and evaluation. (4 votes)	4

Planning data access well in advance to avoid unnecessary costs and delays

7.b was the most relevant solution for the participants. This was also the only solution discussed in this section. The Austrian managing authority explained that planning is most relevant for evaluation purposes. It can be very difficult to plan because you need several steps to clarify in detail which data are needed and from which period. One challenge is that, due to public procurement rules, the managing authority cannot coordinate the evaluation with external evaluators prior to the evaluation.

The Austrian managing authority mentioned the challenge that different data holders define data differently, which reduces the usability of data from administrative registers. It is therefore easier to collect data directly from individuals. The Latvian managing authority agreed with this point and also said that it can be difficult to understand what data are available and whether they are comparable. These challenges make it difficult to plan the evaluations if you cannot coordinate with the evaluators beforehand.

Solution	Votes (relevance)
7.a) Plan well in advance what administrative data will be needed to complement or replace direct data collection for ESF+ monitoring and evaluation.	5
7.b) Managing authorities to coordinate planning with administrative data holders who may know what data is available.	8
7.c) Plan the scope of the data needed to avoid rejections based on a population sample that is too small.	2

8.5. Annex V – ESF/ESF+ and data protection legislations

This annex presents a compilation of documents (in English and original language) related to ESF and data protection laws and rules for all nine countries considered in this study.

While all sources present in this annex we reviewed carefully, it is important to mention that not *all* of these sources were included in the description of national legal frameworks (Section 4 of the main report); only those pieces of legislation that were most relevant in the context of this study were mentioned.

Austria

Document	Original language
ESF Partnership agreement	
Partnership Agreement 2021-2027	Partnerschaftsvereinbarung Oesterreich 2021-2027
Partnership Agreement 2014-2020	Partnerschaftsvereinbarung Oesterreich 2014-2020

Document	Original language
National laws and other rules for the management of the ESF/ESF+ funds	
Operational Programme for implementation of ESF incl REACT-EU 2014-2020	ESF Operationelle Programm Österreich
ESF+ Programme Employment Austria and JTS 2021-2027	DE-ESF+ Programm Beschäftigung Österreich & JTF 2021-2027
Agreement between the federal state and the Laender concerning the control system in Austria for the implementation of operational programmes for the period 2014-2020	Vereinbarung zwischen Bund und den Laendern gemass Art. 15a B-VG ueber das Verwaltungs- udn Kontrollsystem in Oesterreich fuer die Durchfuehrung der opreationellen Programme im Rahmen des Ziels “Investitionen in Wachstum und Beschaeftigung” und des Ziels “Europaeische Territoriale Zusammenarbeit” fuer die Periode 2014-2020
Special Directive of the ministry for labour, social affairs for the implementation of projects under the framework of the ESF 2014-2020	Sonder-Richtlinie des Bundesministers fuer Arbeit, Soziales, und Konsumentenschutz zur Umsetzung von Projekten im Rahmen des Europaeischen Sozialfonds (ESF) 2014-2020
Annex 1a to Special Directive for implementation of projects under the framework of the ESF 2014-2020: Data protection agreement	Anhang 1a zur SRL: Datenschutzvereinbarung
Annex 1b to Special Directive 2014-2020: Information for Data processing	Anhang 1b zur SRl: Information zur Datenvereinbarung
National data protection-relevant laws supplementing GDPR[672]	
Federal Act concerning the Protection of Personal Data (DSG)	
Regulation for the accreditation of certifying bodies	Zertifizierungsstellen-Akkreditierungs-Verordnung
Regulation for the accreditation of monitoring and supervisory bodies	Ueberwachungsstellenakkreditierungs-Verordnung
Regulation on the exemptions from the data protection impact assessment	Datenschutz-Folgenabschaetzung-Ausnahmeverordnung

France

Document	Original language
ESF Partnership agreement	
Partnership Agreement 2021-2027	Accord de Partenariat 2021-2027
Partnership Agreement 2014-2020	Accord de Partenariat 2014-2020
National laws and other rules for the management of the ESF/ESF+ funds	
Decree n° 2014-580 of 3 June 2014 management of European funds 2014-2020	Décret n° 2014-580 du 3 juin 2014 gestion fonds européens 2014-2020

[672] All national laws can be found here. In addition, a list with individual provisions on data protection from other laws (e.g. civil code, employer law, e-commerce-law, registration law, military law, consumer credit law, telecommunication law) can be found here.

Document	Original language
Decree n°2016-126 of 8 February 2016 on the implementation of programmes co-financed by the European structural and investment funds for the period 2014-2020	Décret n°2016-126 du 8 février 2016 relatif à la mise en œuvre des programmes cofinancés par les fonds européens structurels et d'investissement pour la période 2014-2020
Order of 1 April 2016 on the flat-rate pricing of indirect expenditure on operations receiving a contribution from the European Social Fund and the Youth Employment Initiative under national or regional operational programmes mobilising ESF and EYI funds	Arrêté du 1er avril 2016 relatif à la forfaitisation des dépenses indirectes des opérations recevant une participation du Fonds social européen et de l'Initiative pour l'emploi des jeunes au titre des programmes opérationnels nationaux ou régionaux mobilisant des crédits FSE et IEJ
National data protection-relevant laws supplementing GDPR	
Law n°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
Law n° 2018-493 of 20 June 2018 relating to the protection of personal data [amending Law n°78-17 of 6 January 1978]	Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
Law n°2000-321 of 12 April 2000 on the rights of citizens in their relations with administrations	Loi n°2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations
Decree amending law n°78-17 of January 6, 1978 relating to information, files and freedoms	Décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'information, aux fichiers et aux libertés
Ordinance No. 2018-1125 of 12 December 2018 taken in application of Article 32 of Law No. 2018-493 of 20 June 2018 relating to the protection of personal data and amending Law No. 78-17 of 6 January 1978 relating to information technology, files and freedoms and various provisions concerning the protection of personal data	Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel
Law No. 2004-801 of 6 August 2004 on the protection of individuals with regard to the processing of personal data and amending Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms [implementing Data Protection Directive EC/95/46]	Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
Context-specific laws on processing of personal data in the context of labour market and employment (including how and to who data can be shared)	
Civil Code (Article 9)	Code civil (article 9)
Labour Code (Articles L1222-3, L. 1222-4 and L2323-32)	Code du travail (Articles L1222-3, L. 1222-4 and L2323-32)
Criminal Code (Article 226-1 and following; Article 226-16 and following; law of 6 January 1978)	Code pénal (Article 226-1 and following; Article 226-16 and following; loi du 6 janvier 1978)

Germany

Document	Original language
ESF Partnership agreement[673]	
Partnership Agreement 2021-2027	Partnerschaftsvereinbarung der BRD 2021-2027
Partnership Agreement 2014-2020	Partnerschaftsvereinbarung der BRD 2014-2020
National programme of the ESF + (2021-2027)	ESF+ 2021-2027 Bundesprogramm
National laws and other rules for the management of the ESF/ESF+ funds[674]	
Guidelines for the approval of ESF+ resources for the funding period 2021-2027	Fördergrundsätze für die Bewilligung von Zuwendungen aus dem ESF Plus in der Förderperiode 2021-2027
Special ancillary provisions for applications for project funding under the ESF Federal Programme for the European Social Fund Plus	Besondere Nebenbestimmungen fuer Zuwendungen zur Projektfoerderung im Rahmen des ESF-Bundesoprogramms fuer den Europaeischen Sozialfonds Plus
Special ancillary provisions for funding of projects to regional authorities and associations of regional authorities under the Federal ESF Programme for the European Social Fund Plus in the funding period 2021 to 2027	Besondere Nebenbestimmungen für Zuwendungen zur Projektförderung an Gebietskörperschaften und Zusammenschlüsse von Gebietskörperschaften im Rahmen des ESF-Bundesprogramms für den Europäischen Sozialfonds Plus in der Förderperiode 2021 bis 2027)
Rules of procedure of the ESF monitoring committee for the implementation of the ESF federal programme[675]	Geschäftsordnung des Begleitausschusses zur Umsetzung des ESF Plus – Bundesprogramms

Ireland

Document
ESF Partnership agreement
Partnership Agreement 2021-2027 (not yet available)
Partnership Agreement 2014-2020
National laws and other rules for the management of the ESF/ESF+ funds
Circular 13/2015 Management and control procedures for the European Structural and Investment Funds Programmes 2014-2020
ESF Certifying Authority Circular 01/2015: ESF Eligibility Rules that should be read together with the Circular on Financial Management and Control Procedures for the European Structural and Investment Funds (ESIF) Programmes 2014-2020
Circular 08/2015 National Eligibility Rules For Expenditure Co-Financed By The European Regional Development Fund (ERDF) Under Ireland's Partnership Agreement 2014-2020

[673] All funding programmes of the ESF federal programme can be found here.

[674] All funding regulations (Foerderregelungen ESF Plus 2021-2027) can be found here. In addition, more on monitoring and evaluation of the ESF+ can be found here.

[675] Website can be found here.

Document
GDPR-implementing legislation
Data Protection Act 2018
Other relevant legislation
Data Sharing and Governance Act 2019
Statistics Act, 1993
S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.

Italy

Document	Original language
ESF Partnership agreement	
Partnership Agreement 2021-2027	Accordo di Partenariato Italia 2021-2027
Partnership Agreement 2014-2020	Accordo di Partenariato Italia 2014-2020
National laws and other rules for the management of the ESF/ESF+ funds	
Ministry of Economy and Finance Decree 8 June 2022 on National public co-financing from the Revolving Fund under Law no. 183/1987 of the additional REACT-EU resources for the European Regional Development Fund (ERDF) and European Social Fund (ESF) National Operational Programmes 2014-2020, annuality 2021. (Decree No. 1/2022). (22A04539) (OJ General Series No. 186 of 10-08-2022)	Ministero dell'Economia e delle finanze, Decreto 8 giugno 2022 su Cofinanziamento nazionale pubblico a carico del Fondo di rotazione di cui alla legge n. 183/1987 delle risorse aggiuntive REACT-EU per i Programmi operativi nazionali del Fondo europeo di sviluppo regionale (FESR) e del Fondo sociale europeo (FSE) 2014-2020, annualita' 2021. (Decreto n. 1/2022). (22A04539) (GU Serie Generale n.186 del 10-08-2022)
Ministry of Economy and Finance Decree 8 June 2022 on National public co-financing from the Revolving Fund under Law No 183/1987 of additional resources for the Regional Operational Programmes Abruzzo Lazio Marche and Umbria of the European Regional Development Fund (ERDF) 2014-2020. (Decree No 2/2022).	Ministero dell'Economia e delle finanze, Decreto 8 giugno 2022 su Cofinanziamento nazionale pubblico a carico del Fondo di rotazione di cui alla legge n. 183/1987 delle risorse addizionali per i Programmi operativi regionali Abruzzo Lazio Marche e Umbria del Fondo europeo di sviluppo regionale (FESR) 2014-2020. (Decreto n. 2/2022).
Ministry of Economy and Finance Decree No 3 of 16 March 2021 on National public co-financing from the Revolving Fund, pursuant to Law No. 183/1987, for the operational programmes of the European Regional Development Fund (ERDF), the European Social Fund (ESF) for the year 2019 net of the 2019 pre-financing and of the allocation already provided for by Decree No. 20/2020 and for the year 2020, net of the performance reserve. (Decree No. 3/2021).	Ministero dell'Economia e delle finanze, Decreto del 16/03/2021 n. 3 su Cofinanziamento nazionale pubblico a carico del Fondo di rotazione, di cui alla legge n. 183/1987, per i programmi operativi del Fondo europeo di sviluppo regionale (FESR), del Fondo sociale europeo (FSE) annualita' 2019 al netto del prefinanziamento 2019 e dell'assegnazione gia' disposta con decreto n. 20/2020 e annualita' 2020, al netto della riserva di efficacia. (Decreto n. 3/2021).
Decree of the President of the Republic No 22 of 5 February 2018 Regulation laying down the criteria on the eligibility of expenditure for programmes co-financed by the European Structural Investment Funds (EIS) for the 2014/2020 programming period.	Decreto del Presidente della Repubblica 5 Febbraio 2018, n. 22. Regolamento recante i criteri sull'ammissibilita' delle spese per i programmi cofinanziati dai Fondi strutturali di investimento europei (SIE) per il periodo di programmazione 2014/2020.

Document	Original language
National data protection-relevant laws supplementing GDPR	
Legislative Decree No 101 of 10 August 2018, Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).	Decreto Legislativo 10 agosto 2018, n. 101. Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
Legislative Decree No 51 of 18 May 2018, Implementation of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.	Decreto Legislativo 18 maggio 2018, n. 51. Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.
Legislative Decree No 196 of 30 June 2003, Personal Data Protection Code, containing provisions for the adaptation of the national system to Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.	Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
Context-specific laws on processing of personal data in the context of labour market and employment (including how and to who data can be shared)	
LAW No. 300 of 20 May 1970, Rules on the protection of workers' freedom and dignity, trade union freedom and trade union activity, in the workplace and rules on employment (Workers' Statute).	LEGGE 20 maggio 1970, n. 300 (Statuto dei lavoratori). Norme sulla tutela della liberta' e dignita' dei lavoratori, della liberta' sindacale e dell'attivita' sindacale, nei luoghi di lavoro e norme sul collocamento.
Context-specific laws on processing of personal data by the national Tax Agency (including how and to who data can be shared)	
Legislative Decree No 193 of 22 October 2016, Urgent provisions on fiscal matters and for the financing of unavoidable needs.	Decreto Legge 22 Ottobre 2016, n. 193. Disposizioni urgenti in materia fiscale e per il finanziamento di esigenze indifferibili.

Poland

Document	Original language
ESF Partnership agreement	
Partnership Agreement 2021-2027	Umowa Partnerstwa
Partnership Agreement 2014-2020	Umowa Partnerstwa
National laws and other rules for the management of the ESF/ESF+ funds	

Document	Original language
Act of 11 July 2014 concerning rules of implementation of programmes supported from Cohesion Policy in the financial period 2014-2020 (O.J. 2014 item 1146, with later changes)	Ustawa z dnia 11 lipca 2014 o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020
Act of 11 July 2014 concerning rules of implementation of programmes supported from Cohesion Policy in the financial period 2021-2027 (O.J. 2022 item 1079, with later changes)	Ustawa z dnia 28 kwietnia 2022 o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2021-2027
Announcement of the Minister of Development Funds and Regional Policy of December 28, 2021 on the amended guidelines on the conditions for collecting and transferring data in electronic format for the years 2014-2020 (Polish Monitor 2022, item 20)	Komunikat Ministra Funduszy i Polityki Regionalnej z dnia 28 grudnia 2021 w sprawie zmienionych wytycznych w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020
Guidelines on the conditions for collecting and transferring data in electronic format for the years 2014-2020[676]	Wytyczne w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020
Guidelines on the conditions for collecting and transferring data in electronic format for the years 2021-2027[677]	Wytyczne w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2020-2027
National data protection-relevant laws supplementing GDPR	
Act of 10 May 2018 on the Protection of Personal Data (O.J. 2018 item 1000)[678]	Ustawa z 10 maja 2018 o ochronie danych osobowych
Ordinance of 11 May 2015 of the Minister of administration and digitalization concerning the procedures of management of data registries (O.J. 2015 item 719)	Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 w sprawie sposoby prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych
Context-specific laws on processing of personal data in the context of labour market and employment (including how and to who data can be shared)	
Act of 20 April 2004 concerning promotion of employment and institutions of labour market (O.J. 2004 No. 99 item 1001)	Ustawa z dnia 20 kwietnia 2004 o promocji zatrudnienia i instytucjach rynku pracy
Draft Act on employment activities	Projekt ustawy o aktywności zawodowej

Romania

Document	Original language
National data protection-relevant laws supplementing GDPR[679]	
Law no. 190/2018 - Data protection Law on	LEGE 190 18/07/2018

[676] Document approved in November 2021 by the Minister of Funds and Regional Policy.

[677] Document exists only in draft version, not approved and without annexes – this is a similar document to the one above; public comments to this document could be provided until July 2022.

[678] The main act implementing the GDPR (in Polish abbreviated as RODO).

[679] See also Law 179/2022 on open data and reuse of public sector information (transposition of the European Open Data Directive.

Document	Original language
implementing measures of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.	
Law no. 129/2018 – DPA Authority Law on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing (repealing Law no. 677/2001 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data)	LEGE 129 15/06/2018
Law no. 363/2018 – Police and Criminal Justine Authorities Law on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data	LEGE 363 28/12/2018

Spain

Document	Original language
ESF Partnership agreement	
Spanish Partnership Agreement 2014-2020	Acuerdo de Asociación de España 2014-2020
Spanish Partnership Agreement 2021-2027 (first formal version)	Acuerdo de Asociación de España 2021-2027 (primera versión formal)
National laws and other rules for the management of the ESF/ESF+ funds	
Act 50/1985 of 27 December, on regional incentives for the correction of inter-territorial economic imbalances	Ley 50/1985, de 27 de diciembre, de incentivos regionales para la corrección de desequilibrios económicos interterritoriales
Royal Decree 683/2002 of 12 July, governing the functions and management procedures of the European Social Fund Administrative Unit	Real Decreto 683/2002, de 12 de julio, por el que se regulan las funciones y procedimientos de gestión de la Unidad Administradora del Fondo Social Europeo
Royal Decree 899/2007 of 6 July, on regional incentives, implementing Act 50/1985 of 27 December	Real Decreto 899/2007, de 6 de julio, por el que se aprueba el Reglamento de los incentivos regionales, de desarrollo de la Ley 50/1985, de 27 de diciembre
Order ESS/1337/2013 of 3 July, amending Order TIN/2965/2008 of 14 October, determining the expenses eligible for funding by the European Social Fund during the 2007-2013 programming period	Orden ESS/1337/2013, de 3 de julio, por la que se modifica la Orden TIN/2965/2008, de 14 de octubre, por la que se determinan los gastos subvencionables por el Fondo Social Europeo durante el período de programación de 2007-2013
Order ESS/1924/2016 of 13 December, determining the expenses eligible for funding by the European Social Fund during the 2014-2020 programming period	Orden ESS/1924/2016, de 13 de diciembre, por la que se determinan los gastos subvencionables por el Fondo Social Europeo durante el período de programación 2014-2020.
Order HFP/1979/2016 of 29 December, approving the rules on eligible expenditure of the operational	Orden HFP/1979/2016, de 29 de diciembre, por la que se aprueban las normas sobre los gastos subvencionables de los programas operativos del

Document	Original language
programs of the European Regional Development Fund for the period 2014-2020	Fondo Europeo de Desarrollo Regional para el período 2014-2020
Order HAC/114/2021 of 5 February, amending Order HFP/1979/2016 of 29 December, approving the rules on eligible expenditure of the Operational Programs of the European Regional Development Fund for the period 2014-2020	Orden HAC/114/2021, de 5 de febrero, por la que se modifica la Orden HFP/1979/2016, de 29 de diciembre, por la que se aprueban las normas sobre los gastos subvencionables de los Programas Operativos del Fondo Europeo de Desarrollo Regional para el período 2014-2020
Resolution of 22 December of 2021, of the Secretary of State for Social Rights, publishing the Agreement of the Territorial Council of Social Services and the System for Autonomy and Care for Dependency, on the Programming of the European Social Fund Plus, in relation to the objective of combating material deprivation	Resolución de 22 de diciembre de 2021, de la Secretaría de Estado de Derechos Sociales, por la que se publica el Acuerdo del Consejo Territorial de Servicios Sociales y del Sistema para la Autonomía y Atención a la Dependencia, sobre la programación del Fondo Social Europeo Plus, en relación con el objetivo de lucha contra la privación material
National data protection-relevant laws supplementing GDPR	
Spanish Constitution, Art. 18.4	Constitución española, art. 18.4
Organic Act 3/2018 of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
Organic Act 7/2021 of 26 May, on the Protection of Personal Data to prevention, detection, investigation and prosecution purposes of criminal offenses and execution of criminal sanctions	Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales
Royal Decree 389/2021 of 1 June, approving the Statute of the Spanish Data Protection Agency	Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos
Spanish Charter of Digital Rights	Carta de Derechos Digitales
Context-specific laws on processing of personal data in the context of labour market and employment (not exclusively)	
Act 34/2022 of 11 July, on information society services and electronic commerce	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
General Act 11/2022 of 8 June of Telecommunications	Ley 11/2022, de 8 de junio, General de Telecomunicaciones
Royal Decree-Law 14/2019 of 31 October, adopting urgent measures for reasons of public safety in the areas of digital administration, public sector procurement and telecommunications	Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones

Sweden

Document	Original language
ESF Partnership agreement	

Document	Original language
Partnership Agreement 2021-2027	Partnerskapsöverenskommelse
Partnership Agreement 2014-2020	Partnerskapsöverenskommelse
National laws and other rules for the management of the ESF/ESF+ funds	
Ordinance (2014:1383) on the management of the EU Structural Funds	Förordning (2014:1383) om förvaltning av EUs strukturfonder
Act (2007:459) on Structural Funds Partnerships	Lag (2007:459) om strukturfondspartnerskap
Ordinance (2014:1374) on the management of the Fund for European Aid to the Most Deprived	Förordning (2014:1374) om förvaltning av fonden för europeiskt bistånd till dem som har det sämst ställt
Swedish ESF Council regulations and general advice on ESF support under the national social fund programme	Svenska ESF-rådets föreskrifter och allmänna råd om stöd från Europeiska socialfonden inom ramen för det nationella socialfondsprogrammet
Ordinance (2015:61) on State aid within the national social fund programme	Förordning (2015:61) om statligt stöd inom det nationella socialfondsprogrammet
Act (2013:388) on the application of European Union State aid rules[680]	Lag (2013:388) om tillämpning av Europeiska unionens statsstödsregler
Ordinance (2007:907) containing instructions for the Swedish ESF Council	Förordning (2007:907) med instruktion för Rådet för Europeiska socialfonden i Sverige
Archive description of the European Social Fund Council in Sweden	Arkivbeskrivning avseende Rådet för Europeiska socialfonden i Sverige
National data protection-relevant laws supplementing GDPR	
Act (2018:218) containing provisions supplementing the EU Data Protection Regulation	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
Public Access to Information and Secrecy Act (2009:400)	Offentlighets- och sekretesslag (2009:400)
Public Access to Information and Secrecy Ordinance (2009:641)	Offentlighets- och sekretessförordning (2009:641)
Ordinance (2007:975) on Instructions for Swedish Authority for Privacy Protection	Förordning (2007:975) med instruktion för Integritetsskyddsmyndigheten
Context-specific laws on processing of personal data in the context of labour market and employment (including how and to who data can be shared)	
Act (2002:546) on the processing of personal data in labour market policy activities (AF-PuL)	Lag (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten (AF-PuL)
Ordinance (2002:623) on the processing of personal data in labour market policy activities (AF-PuF)	Förordning (2002:623) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten (AF-PuF)
Act (2012:741) on the processing of personal data at the Institute for Employment and Education Policy Evaluation	Lag (2012:741) om behandling av personuppgifter vid Institutet för arbetsmarknads- och utbildningspolitisk utvärdering
Act (2006:469) on the processing of personal data at	Lag (2006:469) om behandling av personuppgifter

[680] Includes obligations on keeping records and publication of specific measures, applicable to the ESF programmes.

Document	Original language
the Inspectorate for Unemployment Insurance	vid Inspektionen för arbetslöshetsförsäkringen
Context-specific laws on processing of personal data by the national Tax Agency (including how and to who data can be shared)	
Act (2001:181) on the processing of data in the Tax Agency's tax activities	Lag (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet
Ordinance (2001:588) on the processing of data in the Tax Agency's tax activities	Förordning (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet
Act (2001:182) on the processing of personal data in the Swedish Tax Agency's civil status registration activities	Lag (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet
Ordinance (2001:589) on the processing of personal data in the Swedish Tax Agency's civil status registration activities	Förordning (2001:589) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet
Act (1998:527) on the State Personal Address Register	Lag (1998:527) om det statliga personadressregistret
Ordinance (1998:1234) on the State Register of Personal Address	Förordning (1998:1234) om det statliga personadressregistret

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

Publications Office
of the European Union