EUROPEAN LABOUR AUTHORITY

Application of the General Data Protection Regulation (GDPR) in exchanging data for risk assessment

GDPR Manual

Contents

Figures

Table

Abbreviations

CJEU	Court of Justice of the European Union
DPA(s)	Data Protection Authority(ies)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
GDPR	General Data Protection Regulation
LED	Law Enforcement Directive
MS(s)	Member State(s)
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
WP29	Article 29 Working Party

1.0 Introduction

This practical manual has been prepared as a follow-up to a training session for analysts on the application of the General Data Protection Regulation (GDPR) in exchanging data for risk assessment related to labour law and social security issues. It serves two purposes. Firstly, it summarises the main legal issues related to the processing and sharing of data for risk assessment under the GDPR as discussed during the training. Secondly, it presents examples from practice or case-law and good practices identified during the online session, as well as through subsequent exchanges with national competent authorities.

In order to make the training as practical as possible, a fictional case study was used to present real-life issues and obstacles that national competent authorities face when processing data for analysis and risk assessment. The details of the case study are presented in Annex I which also includes discussion points. Throughout this manual the examples from the fictional case study are used to illustrate specific legal issues and topics discussed by answering the discussion questions. All such illustrative examples as well as good practices are presented in boxes throughout the text.

This practical manual is structured as follows. Section 1 presents a brief introduction to the history of data protection law and a review of the main legal text governing processing of data for risk assessment, in particular the GDPR. Basic concepts and principles of personal data are elaborated in Section 2, data protection actors are dealt with in Section 3, while Section 4 focuses on data subjects' rights. Section 5 of this manual includes a practical checklist which should be used as a tool to guide national authorities when dealing with the processing of personal data. Finally, the text of the mock case study and the list of most relevant information sources are included in the annexes to the manual.

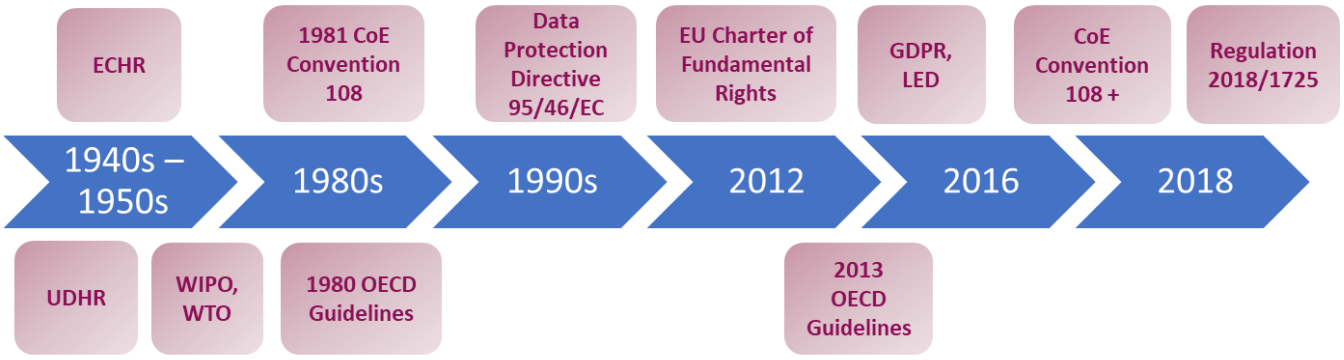
1.1 Brief history of data protection law

The right to personal data protection is a distinct right from the right to privacy (i.e. the right to respect for private life), which emerged in international and European human rights law already in the 1948 Universal Declaration of Human Rights (UDHR) and 1950 the European Convention on Human Rights (ECHR). Data protection laws govern the processing of personal data and give individuals rights with respect to their data. It began in the 1960s-70s as a response to the increase use of computers and the internet and the rise of the information society. Data protection law developed from telecommunication laws and was first discussed at international bodies such as the World Intellectual Property Organization (WIPO), the World Trade Organization (WTO), and the Organisation for Economic Co-operation and Development (OECD), which in 1980 issued first Guidelines (updated in 2013). The first international instrument related to data protection was the Convention for the protection of individuals with regard to automatic processing of personal data (**Convention 108**) adopted by the Council of Europe in 1981. Modernised in 2001 and 2018, Convention 108+ is still the only legally binding international instrument in the field of data protection.

As data protection cuts across many different legal areas and policies, the first EU legal document was only adopted in 1995 in the form of a directive. The **Data Protection Directive 95/46/EC** was a principle-based directive that also contained data subjects' rights and created national Data Protection Authorities (DPAs). However, with the emergence of new technologies, the Data Protection Directive became outdated and from around 2012 onwards a real push was made to make Europe fit for the digital age.

The **General Data Protection Regulation - GDPR** (Regulation 2016/679) was adopted in May 2016 and has been applicable since 25 May 2018. It regulates the right to the protection of personal data stipulated in Article 8 of the **EU Charter of Fundamental Rights**.

Figure 1: Timeline



1.2 Legal framework

The GDPR pursues two goals:

- to protect natural persons with regard to the processing of their personal data (**fundamental right**) and
- to support the **free movement** of such data (**economic aspect**).

It applies to entities processing personal data (both private and public) in the EU/EEA and in some cases also to those located outside the EU/EEA area. The GDPR is a regulation and therefore uniformly and directly applicable in all Member States.

The data protection package adopted in May 2016 also included the Law Enforcement Directive – LED (Directive (EU) 2016/680). As this Directive protects citizens' fundamental right to data protection whenever personal data are used by criminal law enforcement authorities for law enforcement purposes, it is not applicable to national competent authorities when exchanging data for risk assessment related to labour law and social security issues.

A separate legal text – Regulation 2018/1725 sets forth the rules applicable to the processing of personal data by European Union institutions, bodies, offices and agencies.

Although the GDPR is directly applicable in the Member States (MSs), it often acts as 'enabling legislation' leaving considerable national discretion in relation to public sector data processing. Apart from adopting national GDPR-implementation laws, each MS also has sectorial laws, and dataset-specific laws that govern the processing of personal data with respect to specific areas, databases etc. Such laws could already exist pre-GDPR or could have been amended thereafter.

Whilst all these national laws should be taken into account when processing personal data for risk assessment related to labour law and social security issues, ***this manual does not intend to provide any legal guidance or advice on national legal systems****.*

2.0 Basic concepts and principles of data protection

2.1 What is personal data and what is not?

Personal data is **any information relating to an identified or identifiable natural person** (Article 4(1) GDPR). Although the GDPR does not address data of legal persons, it may cover information related to companies in cases where it can be linked to an individual (e.g. John Smith Ltd.).

A person can be identified directly or indirectly, in particular by reference to **an identifier** (such as name, ID number, age and date of birth, address, phone number, email address, gender, marital status, photograph, online identifier such as IP address, location, etc.) or to **one or more factors** specific to the physical, physiological, genetic, mental, economic, cultural or social identity. If the data allow singling out an individual in a group through a combination of different data point which alone might not be personal, such data are considered personal data.

Example 1: CJEU Nowak and Breyer cases

Mr Nowak is a trainee accountant who failed an open book examination for the fourth time. When he made a request for access to his personal data, the Institute of Chartered Accountants of Ireland refused to send him his exam scripts, arguing that these were not personal data. The CJEU ruled that written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute personal data.

Mr Breyer is a German activist who accessed several publicly available governmental websites. In order to prevent attacks, these websites store information on all access operations in log files, including the IP address of the computer that accessed the website. In this case, the CJEU stated that even a dynamic IP address registered by online media service providers, when a person accesses a website, constitutes personal data, if the provider has the legal means to obtain additional data related to that person from the internet service provider, thus being able to identify the data subject.

In order to consider that the data “relate to” an individual, one of the following three elements, in particular the content one, should be present:

- content (Data about a person)
- purpose (What is the outcome?)
- result (Can the use of data have an impact on a person’s rights?)

Under certain circumstances even the following types of data could be considered as personal data: service history of a person’s vehicle, letter sent by an insurance company to an insured person, data collected by an electronic water metre about water use in an apartment, a house evaluation if it can be linked to an individual owning the house or

	living in it, call log of a telephone, information contained in the minutes of a meeting, which cover certain aspects on an individual).

Anonymous data is any information relating to a natural person where the person can no longer be identified. However, even completely anonymised databases might contain enough data points to ultimately allow identification of an individual. **Aggregated statistics, ratios, percentages etc. are not personal data as long as the sample group is large enough**.

Where personal data relate to the health, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, or biometric data of an individual, they are considered a **special category of personal data ("sensitive personal data")** for the purposes of GDPR (Article 9(1)). This may even include data that inadvertently reveal one of these aspects, such as attendance at a particular health clinic or religious event, dietary preferences, etc. These data merit specific protection as they are by their nature particularly sensitive, or their processing could create significant risks to the fundamental rights and freedoms (it is interesting to note that financial data, for instance, are not on the list).

	*Photographs are covered by the definition of biometric data only when processing through specific technical means allowing the unique identification or authentication of a natural person (e.g. facial recognition).*

Example 2: Fictional case study – defining the types of data

The Analysis and Intelligence Unit of the Labour Inspectorate has requested the following information from the Ministry for Social Protection: name and surname, sex, ID number / passport number, date of birth, nationality, address, name and seat of the employer, party for whom the services are provided, location of work, period of posting (number of days), remuneration / basic monthly salary (in EUR), other monthly allowances (in EUR), unemployment benefits received in 2022, victim of an accident at work in 2022.

Data such as name and surname, sex, ID number / passport number, date of birth, nationality, address are identifiers based on which an individual can be directly or indirectly identified, hence constitute personal data (**content element**). Information identifying a person as a victim of an accident at work in 2022 is not only personal data but sensitive personal data. Furthermore, even information regarding the period of posting (number of days), remuneration / basic monthly salary (in EUR), other monthly allowances (in EUR), and unemployment benefits received in 2022 are personal data as such data give information about the specific situation of an individual and will likely be used to evaluate, treat in a certain way, or influence a status or behaviour of an individual (**purpose element**). E.g. individuals with longer posting periods and salary below the minimum level might be scrutinised more intensely. Finally, even the name and the address of the employer / a third party and the location of work can be seen as personal data, if such data will be used to have an impact on a certain person's rights and interests (**result element**). E.g. such information might be personal data of the employer and also relate to the individuals working for a certain employer on a specific

construction site as it puts them at a concrete place at a specific time and might lead to further investigations int their employment relationship.

2.2 What is processing?

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 (Article 4(2) GDPR).

Processing includes almost any activity related to personal data 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 (it basically covers most operations involving personal data).

For GDPR to apply (i) data have to be processed by **automated means** (e.g. computer, smart phone, tablet), without human intervention; or (ii) in case data are not processed by automated means, such data have to be (or are intended to be) part of a **filing system** (e.g. structured paper files, posted notes or similar whether centralised, decentralised or dispersed – Article 4(6)).

The GDPR does not apply if the processing is outside the scope of EU law (i.e. activities which concern national security or are related to the common foreign and security policy of the EU) or in case it takes place in a purely personal or household activity.

Example 3: Fictional case study – defining the processing operations

All activities of the Analysis and Intelligence Unit of the Labour Inspectorate such as requesting certain data, obtaining data in electronic and physical form (USB key), storing data, extracting information from Excel files and the USB key, analysing data, creating new Excel files, placing Excel files in a cloud, deleting unnecessary data, sending data to the undertakings, receiving additional data, sending data or enabling access to data to the Health and Safety Unit etc. are considered to fall under the definition of processing.

2.3 Basic principles

Figure 2: Basic principles (Article 5 GDPR)

Lawfulness, fairness and transparency

The principle of lawfulness (Article 5(1)(a) GDPR) is one of the central principles of data protection. It requires that there has to be a specific **legal basis** for each processing of personal data. This principle also requires that the processing must be **fair** (defined in the negative, meaning that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected, misleading) and **transparent** (provision of comprehensive and clear information to the data subject).

Purpose limitation – Why are we processing?

The controller must collect data **for specified, explicit and legitimate purposes** and must not further process the data in a manner that is incompatible with the purposes for which they were collected (Article 5(1)(b)). This is one of the key data protection principles. It requires that the **purpose of processing** must be determined when a processing operation is designed, as this will also set out which data are needed to achieve this purpose. Any **further processing** needs to be assessed on a case-by-case basis and is only allowed if an additional purpose is compatible with the original one. The controller needs to perform a **purpose compatibility test** as such further processing should not create additional risks for the rights and freedoms of data subjects. To this end, one needs to look at: (i) the link between initial and 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.

Example 4: CJEU case - Hungarian internet and TV provider

In a recent case, the CJEU needed to decide whether a Hungarian internet and TV provider breached the principle of purpose limitation by moving their customer database into a test database to repair a

technical error. The Court ruled that the principle of purpose limitation does not prevent such use of previously collected and stored personal data, since this further processing (fixing a technical problem) is compatible with the specific purposes for which the personal data was initially collected (providing TV and internet services) and customers could expect such further processing.

Example 5: Fictional case study – defining the purpose

The Analysis and Intelligence Unit of the Labour Inspectorate is interested in the analysis of information related to the working time and remuneration of some construction workers that are currently posted in their territory. This could help the authority to tackle specific social dumping practices. Data requested are needed to target companies at risk of non-compliance.

These purposes are rather vague and far-reaching and do not really allow to pinpoint exactly what is the aim of the data collection. They should be made more concrete, specific and explicit. From the information above, it is not sufficiently clear whether the intention is to conduct a general analysis of the extent of social dumping practices in case of posted workers in the construction sector or whether specific inspections are planned to discover concrete cases of non-compliance. The Unit should first specify the purpose of each processing and then explain why it needs certain data to achieve that purpose.

Good practice 1: Avoiding the collection of unnecessary data

In the context of inspections, national competent authorities should request only those data they need for the intended purpose (why do you need the information). In order to prevent employers or public entities from transferring data that were not requested or are not needed for the purpose, national competent authorities could use pre-defined forms which specify exactly which data or documents are needed. Any superfluous data that is not needed for the purpose of processing should be immediately deleted (destroyed, blackened, returned etc.).

Additional data could however be kept and reused if the national competent authority is able to establish a legal basis and a purpose for this processing. Such further purpose must be clearly stated and compatible / closely related to the initial one.

Data minimisation and proportionality – What exactly do we need for our purpose?

Only personal data that is adequate, relevant and limited to what is necessary in relation to the purpose shall be processed (Article 5(1)(c) GDPR). The principle of **data minimisation** forces controllers to only collect data that is directly relevant and necessary to accomplish a specified purpose at the time of collection (“need to know, instead of nice to have”). It also means that data should only be retained for as long as it is necessary to fulfil that purpose.

Example 6: National Data Protection Authorities (DPAs) cases - swimming pool, hotel

The APD/GBA (Belgian DPA) ordered a controller, a vacation park owner, to comply with the principle of data minimisation pursuant to Article 5(1)(c) GDPR. The controller processed personal data to

prevent the fraudulent abuse of a swimming pool discount card for family members, but unnecessarily requested photos and degree of kinship of the data subject's family members when their names alone would have sufficed.

The AEPD (Spanish DPA) ruled that a hotel that scanned guests' passports for identification purposes was not compliant with the principle of data minimisation. When guests checked into the hotel, their passport was scanned as part of the registration process. The passport scan included more personal data than what was required for the purpose. Collection of an ID number, for example, would have been sufficient for identification.

Example 7: Fictional case study – defining the amount of data

When the Analysis and Intelligence Unit of the Labour Inspectorate decides which data it should request, only data that are necessary with respect to the specified purpose should be requested. It should for example be justified why data on gender are needed. If this question cannot be answered referring to one of the purposes of processing, then such data should not be collected. The same is true for the ID/passport number or the date of birth. If one such identifier is enough, the controller cannot process additional data, to have them “just in case”.

A similar rule applies when the Unit decides which data should be transferred in the summons sent to the undertaking. The controller should always start with the minimum amount of data to fulfil a purpose. If this does not suffice to identify a person, more data could be revealed (step-by-step approach).

Good practice 2: Dealing with court requests

The national court requested from the Labour Inspectorate information about 34 persons although the court case only covered one person. The Labour Inspectorate is obliged by national law to cooperate with judicial authorities; however, it seemed that the court’s request was excessive in light of the data minimisation principle. Before responding, the Inspectorate should consult its Data Protection Officer (DPO) and not simply transfer all data without further consideration. In order to demonstrate compliance with data protection principles, the Inspectorate could also ask the court for further clarification as to why the data of the remaining 33 persons are also necessary for the processing purpose and document such correspondence. Upon reassurance by the court that the data protection principles had been followed, the Inspectorate could then transfer the files.

Accuracy – Making sure that the data is correct

Data need to be **correct**, **kept up to date** and all reasonable steps should be taken to **delete or rectify inaccurate data** promptly (Article 5(1)(d) GDPR). The need for data accuracy is a consequence of the more general principle to correctly represent a person at the most diverse levels and in the most diverse contexts and is one of the essential prerequisites of the right to informational self-determination (recital

39). It applies not only to facts that are processed about a person, but also to value judgements, in particular forecasts and correlations.

Example 8: Fictional case study – defining the accuracy of data

In order to make sure that data are correct, the Analysis and Intelligence Unit of the competent enforcement authorities could cross-check such data at regular intervals against information in other public databases or ask enterprises to confirm their accuracy before processing.

Data retention (storage limitation) – How long will we keep the data?

Data should be kept in a form which permits identification of data subjects for **no longer than it is necessary** for the purposes for which the personal data is processed (Article 5(1)€ GDPR). To limit how long personal data should be kept is also part of data minimisation ("as long as necessary, as short as possible"). Longer storage is allowed in case of processing for archiving purposes in the public interest, scientific or historical research or statistical purposes.

EU or national legal rules often impose fixed retention periods. In the absence of such rules, the controller needs to specify retention periods, stemming from the purpose of processing. Note that retention periods can differ among processing purposes for the same data set.

Example 9: Fictional case study – defining the retention periods

The Unit should check with the help of their Data Protection Officer the EU and national legislation applicable to competent enforcement authorities and legislation covering infringement of labour rules (e.g. in particular retention periods for personal data related to infringements of national labour rules). In the absence of specific legislation, the Unit needs to determine its own retention periods, ideally in the form of a comprehensive retention plan covering all processing operations.

Data security (integrity and confidentiality) – How can we keep the data safe against the risk of interference?

Personal data should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures (Article 5(1)(f) GDPR). It is the responsibility of the controller (and the processor if one is used) to ensure **confidentiality** (e.g. only authorised staff should have access to the data necessary for their processing tasks), **integrity** (e.g. necessary information security so data cannot be tampered with) and **availability** of data (Article 24(1) GDPR).

Data protection by design and by default aims at integrating privacy and data protection considerations into processing operations, e.g. into the design specifications and architecture of information and communication systems and technologies (such as automatic deletion after elapse or retention period), in order to facilitate compliance with data protection principles (Article 25 GDPR).

Example 10: Fictional case study – ensuring data security

The Enforcement Authorities should put in place appropriate technical and organisational measures to secure data stored electronically (e.g. password protection, clear screen policy, access control, logs, antivirus and malware protection, regular back-ups, etc.) or in paper files (e.g. clear desk policy, video surveillance, usage of locks and access badges, etc.). A USB key with documentation should be password-protected and stored in a secure area, for instance in a dedicated cupboard which can be locked. If files are stored on a cloud, a cloud provider should also put in place appropriate measures and should not store data outside the EU/EEA space.

Security should also be ensured if/when transferring data to other Units within the Inspectorate or to third parties in the same Member State or in the EU/EEA area. In case of intra-EU transfers, the information exchange could be done using secured EU information exchange systems such as the Internal Market Information System (IMI), the Electronic Exchange of Social Security Information (EESSI), or the European Register of Road Transport Undertakings (ERRU).

Accountability

Accountability is directly addressed to the controller (either public or private entity). The controller is **responsible for ensuring compliance** with data protection principles and obligations as stipulated in the GDPR and to be **able to demonstrate compliance** both to individuals and to the DPA on an **ongoing basis**. The principle of accountability requires documenting compliance and being able to provide such documentation upon request to the competent DPA (concept of proactive and demonstrable compliance).

Putting the accountability principle into effect means that national competent authorities understand their obligations under GDPR and comply with them. It is important to liaise with the DPO and to follow check lists as well as set up policies and procedures, which should also be continuously reviewed.

2.4 Legal bases

The need for a legal basis is one of the backbones for the lawfulness of processing operations and is an essential element of the principle of fair processing. The GDPR requires that any entity (private or public) or an individual processing personal data must do so based on one of the six legal bases:

- data subject's consent (Article 6(1)(a))
- processing is necessary for the preparation or performance of a contract to which the data subject is a party (Article 6(1)(b))
- processing is necessary for compliance with a legal obligation to which the controller is subject (Article 6(1)(c))
- processing is necessary to protect the vital interests of the data subject or another person (Article 6(1)(d))

- processing is necessary for the performance of a task in the public interest, or the exercise of official authority vested in the controller (Article 6(1)I)
- processing is necessary for the legitimate interests of the controller, provided those interests do not override the rights of the data subject (Article 6(1)(f)).

*The list of possible legal bases in GPDR is **exhaustive** (closed list) and there is **no hierarchy** between the legal bases, meaning that in order for processing to be lawful, personal data must be processed on one or more legal bases as provided for in Article 6(1) GDPR. The variety of legal bases should in principle suffice to legitimise all possible processing operations.*

Public interest and legal obligation

The most appropriate legal bases underpinning the processing of personal data by national competent authorities for risk assessment related to labour law and social security issues, are public interest and legal obligation.

For a controller to rely on the legal basis under **Article 6(1)(e) GDPR,** the processing should be **necessary for the performance of task carried out in the public interest** or in the **exercise of official authority vested in the controller** (see also recital 45). This legal basis allows for a broad interpretation as the public interest processing does not have to be expressly laid down in a legal basis; however, it should be described in a specific and clear manner. Although typically official authority or public tasks will have been attributed in statutory laws or other legal regulations, they can also be derived from the mandate of a public body.

Example 11: The Luxembourg Labour and Mines Inspection' case

The Luxembourg Labour and Mines Inspection requested an employer to provide information about its employees in the context of an inspection such as working time records, work permits, medical certificates etc. The Inspection is a public body tasked with supervisory authority to conduct controls and examinations and to that end request documents based on national law. The employer rejected the request stating that due to data protection rules, it could not provide the requested information. The court ruled against the employer as the Inspection had a clear legal basis (either a legal obligation or a public interest).

Article 6(1)(c) GDPR can only be relied upon if processing is **necessary for compliance with a legal obligation to which the controller is subject**. The legal obligation should be laid down in EU or MS law and should be sufficiently clear, precise and foreseeable (recital 41). For a legal obligation to be a valid legal base it should also determine the purpose of processing, meet an objective of public interest and be proportionate to the legitimate aim pursued (Article 6(3)).

Legal bases in Article 6(1)(c) and Article 6(1)(e) enable further discretion by EU or MS law (Article 6(2) and (3)). When enacting more specific (sectorial) legislation EU or national legislators need to consider the fundamental rights or interests of data subjects

	and perform a necessity test. Such laws cannot go beyond the rules set out in the GDPR and create other or different legal bases.

Example 12: Fictional case study – defining the legal basis

Most probably the Labour Inspectorate can analyse the extent of social dumping practices in the construction sector based on its mandate (e.g. to supervise conformity with EU and national labour legislation). The purpose of inspection supervision in case of non-compliance is, however, most probably defined in national law.

Other legal bases

Other legal bases seem less suitable for the processing of data by public authorities such as national competent authorities working on analysis and risk assessment.

The legal basis of **legitimate interests** in Article 6(1)(f) GDPR is normally out of reach for public authorities when they are carrying out their tasks (Article 6(1) last sentence). Hence, national competent authorities that are processing data for risk assessment cannot rely on this legal basis.

Similarly, it would not be suitable to rely on legal bases linked to a **contract** (Article 6(1)(b) GDPR) or **vital interests** (Article 6(1)(d) GDPR). For the former legal basis to apply, one of 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. Considering the nature of the relationship between data subjects and the competent authorities it is not possible to claim that the processing of individuals' personal data is resulting from the necessity to perform contractual obligations towards data subjects or to enter into a contract with them. Regarding the latter legal basis, vital interests of the data subject or another person can only be used where the life of an individual is in danger, enabling him or her to provide consent for processing (recital 46).

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 as consent must be freely given, specific, informed, and unambiguous (Article 4(11) GDPR). Furthermore, under Article 7 GDPR consent must be requested in a transparent and fair way (Article 7(2) and should be withdrawable at any time (Article 7(3)). The EDPB Guidelines suggest that consent is unlikely to be an appropriate ground for processing of personal data by public authorities as there is often a clear imbalance of power in the relationship between the controller and the data subject. In such a situation, it cannot be expected that consent was indeed freely given. Lastly, the fact that consent **can be withdrawn** at any time makes it a rather unstable legal basis.

Special categories of personal data

Processing of special categories of personal data (sensitive data) is in general prohibited (Article 9(1) GDPR), unless the controller can base its processing on one of the **10 grounds for lifting the prohibition** in Article 9(2) GDPR. Similarly, as in the case of general legal bases, the list of legal bases

in Article 9 is **exhaustive** and broad enough to be able to cover the need to process sensitive personal data.

Whether processing of sensitive personal data requires both a ground under Article 9 GDPR and a legal basis under Article 6 GDPR has been a matter of debate. When processing sensitive personal data, all general principles and rules of the GDPR apply as well, including the condition for lawful processing and **in principle also the need to have a legal basis**. In case where grounds in Article 9 correlate with legal bases in Article 6, while offering to data subjects an even stricter and better protection (i.e. legal ground of *explicit* consent; vital interest of a person *physically or legally unable to give consent*; and *substantial* public interest), such grounds subsume the corresponding legal basis and do not require an additional correlation. On the contrary, all other grounds (i.e. necessary in the field of employment and social security and social protection law; legitimate activities of foundations, associations or other NGOs; personal data which are manifestly made public by the data subject; necessary for the establishment, exercise or defence of legal claims; necessary for the purposes of preventive or occupational medicine; necessary for reasons of public interests in the area of public health; and necessary for archiving in the public interest, scientific or historical research or statistics) also require an additional legal basis pursuant to Article 6(1) GDPR.

Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health (Article 9(4) GDPR).

3.0 Data protection actors

3.1 Data subject

A data subject is a **natural** person (Article 4(1) GDPR).

The GDPR applies only to living data subjects and not to deceased persons (recital 27). However, MSs may provide alternative rules for the protection of deceased persons which is usually achieved through further data protection, constitutional or personality rights.

3.2 Controller

A controller is a **natural or a legal person**, public authority, agency or other body who **alone or jointly** with others **determines** the **purposes** and **means** of the processing of personal data (Article 4(7) GDPR).

The responsibilities of the controller are defined in Article 24 GDPR. Accordingly, controllers need to be able to demonstrate that any processing of personal data performed on their behalf is in accordance with the GDPR (accountability principle).

Since the responsibilities stemming from the GDPR focus on the controller it is essential to determine who this is.

A controller could be determined either by law (**legal competence**) or by **factual influence** (the one who initiates and determines the processing). Controllership is a functional concept; it aims to allocate responsibility where functional control is being exercised (without the controller the processing would not take place). This means that the factual situation needs to be analysed to ensure that responsibility is placed exactly where control can be exerted.

Example 13: Fictional case study – defining the controller

The Analysis and Intelligence Unit of the Labour Inspectorate, hence the Labour Inspectorate, is the one who determines the purposes of processing (e.g. analysis of the extent of social dumping practices in the construction sector and inspection and supervision activities to check compliance) as well as the means (e.g. obtaining data from the Ministry of Social Protection and from undertakings by sending formal notifications).

The controller is the entity who determines the **purposes (why?)** and **means (how?)** of processing. The former element is the most important as the determination of purposes automatically triggers controllership. However, the determination of means, in particular with respect to technical or organisational questions, is in practice often left to the data processors. A distinction should be made between essential means (decided by the controller) and non-essential means, for example the exact type of hardware or software or the technical and organisational means to be used (can be decided by the processor).

Joint controllership (co-controllers)

Joint controllership is limited to those operations for which joint controllers effectively co-decide on the means and purposes of the processing of the personal data (Article 26(1) GDPR). It is possible that one controller is dominant and another one only dealing with some parts of processing operations.

The concept of joint controllership **requires a (public) determination of respective responsibilities** for compliance with data protection law (e.g. who should respond to data subjects' access requests and react to subjects exercising their rights, who is in charge in case of a data breach, or decides how to design data security). Such a contractual arrangement needs to be transparent and legally binding but can take any legal form. The essence of the arrangement needs to be made available to data subjects (Article 26(2) GDPR).

Example 14: CJEU Jehovah's witnesses' case

In this landmark case about joint controllership, the CJEU needed to determine whether Jehovah's witnesses are exempt from data protection rules when gathering data during their visits to potential converts. The Court noted that the group keeps a list of people who have asked not to be contacted, known as a "refusal register", as well as "the name and addresses of persons contacted, together with information concerning their religious beliefs and their family circumstances". In this context, the Court clarified that the joint responsibility of several actors can differ across the process and that they do not even have to have access to the data. Those actors may be involved at different stages of a processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case. As a consequence, the Court ruled that individual Jehovah's witnesses were joint controllers together with their organisation and that the GDPR was applicable to them.

3.3 Processor

A **processor** is a natural or legal person, public authority, agency or other body which processes personal data **on behalf** of the controller (Article 4(8) GDPR).

The responsibilities of a processor are covered in Article 28 GDPR. Whereas the controller determines the processing operation (the why and the general how), it does not usually have the technical or organisational expertise to conduct such operations. A processor is a separate legal entity that supports the data controller when processing personal data (**service provider**) and is bound by the instructions given by the controller.

In some instances, the traditional role and professional expertise of a service provider may play a predominant role which may qualify it as controller (e.g. accountants, lawyers, insurers).

The controller remains liable for all processing undertaken by the processor, even if it is unlawful, except when a processor does not follow the instructions of the controller and acts in its own interest or processes personal data for further purposes. In such a case, the processor will be considered as a controller in its own right.

Processing by a processor must be governed by a contract (**data processing agreement**) or another legal act under EU law that is legally binding on the processor. Such a data processing agreement should: (i) include the essential elements of the processing (for example its subject matter, duration, nature and purposes, type of personal data, categories of data subjects, obligations and rights of the controller vis-a-vis the processor, the need for documented instructions, confidentiality, security of the processing); (ii) govern the duty of the processor to provide assistance to the controller in ensuring compliance with the GDPR; (iii) limit further processing by sub-processors; (iv) specify duties and rights of the controller to carry out audits and inspections (Article 28(3) GDPR).

A special form of the processor is the "**sub-processor"** engaged by the processor which requires another processing agreement and authorisation through the controller (Article 28(2)-(4) GDPR). In all instances, however, the controller remains responsible for data protection compliance even if the processing is undertaken by a processor and a chain of sub-processors. It is therefore vital to have influence on this chain of various processing agents via contractual clauses.

Processing in the cloud

Cloud computing is the on-demand availability of computing resources as services over the Internet. As providers of cloud computing services are getting increasingly powerful and can determine to a large extent the contents of processing agreement. Therefore, the debate is on-going whether such providers should be considered as joint controllers or even controllers in their own right concerning certain processing operations (for example the processing of meta-data by providers such as Microsoft).

Guidance from the Danish Data Protection Agency - Datatilsynet (see also Annex II for more information) provides a checklist to consult in order to determine what a cloud service provider really does with personal data stored entrusted to it.

Controllers, joint controllers and processors are **jointly liable** to data subjects for mistakes during the data processing operations, unless they can prove they are not in any way responsible for the event giving rise to the damage (Article 82 GDPR).

It is important to look at the factual situation as various combinations are possible. Who has the "decisive influence" on the processing of personal data, is there an instance of joint controllership, has a processor engaged a further processor (sub-processing) etc. For this reason, controllers ned to check the data flows and to identify what roles the identified entities play.

3.4 Data Protection Officer (DPO)

The data protection officer (DPO) is a natural or legal person who assists the controller and/or the processor in ensuring compliance with the GDPR. **Public authorities are obliged to appoint a DPO** (Article 37(1) GDPR). Private entities need to appoint a DPO if their core activity entails large-scale regular and systematic processing of personal data or large-scale processing of sensitive data (e.g. a

hospital). A possibility exists to share a DPO among several public authorities or bodies, taking into account their organisational structure and size (Article 37(3) GDPR).

The DPO shall be designated on the basis of professional qualities, in particular expert knowledge of data protection law and practice. The necessary level of expert knowledge depends on the data processing operations carried out, the complexity and scale of data processing, the sensitivity of the data processed, and the protection required for the personal data processed (Article 37(5) and recital 97).

The function of a DPO is a cornerstone of the accountability-based compliance framework. The DPO acts as an intermediary between relevant stakeholders (e.g. DPAs, data subjects, and departments within a public body) and has the following tasks (Article 39 GDPR):

- inform and advise controller/processor and employees
- monitor compliance with the data protection law and internal rules and regulations regarding data protection
- provide advice on data protection impact assessments (DPIA)
- cooperate with the DPA.

The controller and the processor should ensure that the DPO is **involved properly and in a timely manner** in all data protection issues (Article 38(1) GDPR – early and meaningful involvement). The position of the DPO should be **independent**, meaning that the DP does not receive instructions regarding the execution of tasks. The DPO should report to the highest management level and should not be subject to situations of conflict of interests (Article 38(3) GDPR– for example a DPO also acting as the Head of IT or as the compliance officer). The DPOs are not liable for non-compliance of the controller with the GDPR but only for the quality of their own advice.

3.5 Data Protection Authority (DPA)

MSs must provide for one or more independent DPA to **monitor GDPR application**, protect fundamental rights and facilitate free data flow (Article 51(1) GDPR).

Although most MSs have one DPA, federal states might have several ones. For instance, Germany (Federal + one DPA for every Land, whereby Bavaria has two authorities) and Spain (National + two regional authorities in Catalunya and País Vasco).

The DPA should be **independent**, meaning that it should be free from any direct or indirect external influence.

One of the main tasks is also to **handle complaints** lodged by the data subjects and to **investigate**, to the extent appropriate, the subject matter of the complaint. The DPA can issue warnings to order compliance, impose a temporary or definitive ban and administrative fines.

European Data Protection Supervisor (EDPS)

The EDPS monitors and ensures compliance by EU institutions, bodies, offices and agencies. Its duties are laid down in the Regulation (EU) 2018/1725.

European Data Protection Board (EDPB)

The EDPB is an independent European body which contributes to the consistent application of data protection rules throughout the EU. Its task is to promote **cooperation** between the national DPAs.

The EDPB was established by the GDPR, and is based in Brussels. Its predecessor was the Article 29 Working Party (WP29). The EDPB is composed of representatives of the EU national DPAs, the EDPS, and the DPAs of the EFTA EEA States (Iceland, Lichtenstein, Norway). The European Commission and the EFTA Surveillance Authority have the rights to participate in certain matters as observers.

The EDPB and the EDPS issue on their websites advice in the form of guidelines, opinions, and decisions that can provide a reliable and clear interpretation of the rules in the GDPR. Some of the most important documents, together with the hyperlinks, are listed in Annex II.

4.0 Rights of data subjects

4.1 Transparency

Transparency is a long-established feature of EU law and is an expression of the **principle of fairness**. If individuals do not know that their data are being processed, they cannot check whether the processing is lawful and exercise their rights.

A controller needs to be transparent vis-à-vis data subjects, meaning that it should provide the data subjects with the following **information**: (i) the identity and the contact details of the controller, (ii) contact details of the DPO, (iii) purpose and legal basis of the processing, (iv) categories of personal data processed, (v) recipients of personal data, (vi) transfers of personal data outside the EU/EEA, (vii) retention periods, (viii) use of the legitimate interests as a legal basis, (ix) how to exercise data subjects' rights, (x) how to lodge complaints with the DPA, (xi) the source of the personal data, and (xii) whether automated decision-making is taking place (Articles 12, 13 and 14 GDPR).

*Information is usually provided to an individual in the form of **privacy notices, privacy statements** or similar forms which should be easily available on the website of the controller.*

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. understood 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).

If the personal data are collected from 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 period 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).

The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. The challenge is to make data subjects understand in non-technical language what is happening with their data.

Several **exceptions** to the obligation to provide information exist such as: (i) when a data subject already has the information; (ii) the provision of information proves impossible (e.g. the controller does not have contact details of data subjects), would involve a disproportionate effort (however, informing people via their postal address is not considered to be a disproportionate effort) or would render impossible or seriously impair the achievement of that processing (e.g. money laundering investigations); (iii) obtaining or disclosure is expressly laid down by EU 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 (iv) where

personal data must remain confidential subject to an obligation of professional secrecy (e.g. medical secrecy).

Example 15: Spanish DPA case - a pub

A sign informing data subjects about the video surveillance in front of a pub in Spain was stolen three times. Upon complaint of a data subject that the pub did not comply with the obligation to provide information, the Spanish DPA did not fine the controller (the pub) as they had showed their willingness to comply with transparency obligation and had already replaced the missing sign at last three times, including once on the same day the complaint was filed.

Example 16: Fictional case study – informing data subjects

Firstly, the Analysis and Intelligence Unit would need to check with the Labour Inspectorate DPO what types of privacy policies exist within the Labour Inspectorate and where are they saved. Secondly, with the help of the DPO, the Unit would need to see if the obligation to provide information to data subjects even exists and if any of the exceptions could be applied (for instance in case of inspection supervision obtaining or disclosing data might be expressly laid down by national law, removing the obligation to inform the individuals). If no exception to the transparency obligation could be established, the Unit would need to inform individual data subjects (e.g. by sending them an email, regular mail).

4.2 Rights of data subjects

GDPR expands and enacts new rights of data subjects, all with the aim of enabling their control over personal data.

Right of access

Data subjects have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed and where that is the case, **access to the personal data and related information** (Article 15(1) GDPR). The right of access serves the purpose of guaranteeing the protection of the data subjects' rights to privacy and data protection and may facilitate the exercise of rights flowing from it.

The right to access entails **all data** that the controller holds about the data subject, for example: sensitive personal data, personal data related to criminal convictions, data knowingly and actively provided by the data subject, observed data or raw data (e.g. transaction history, activity logs such as access logs, history of website usage, location data, handwriting, keystrokes), data derived from other data (e.g. credit history, classification, residence derived from postcode), data inferred (e.g. profiles build about an individual, credit scores, algorithmic results, results of health assessment, personalisation), and pseudonymised data.

Information about the processing includes: confirmation of processing, purpose, categories of data processed, recipients, retention period, data subject rights, including the right to complain to the DPA, source of the data, in case of automated decision-making, information on the logic involved, and in case of intended transfers outside the EU/EEA space, information about safeguards.

Text modules of privacy notice and record of processing can be recycled, but have to be tailored to the specific request for access, e.g. regarding information on recipients, and have to be as concrete as possible.

The controller needs to provide a copy of the personal data undergoing processing. However, access can also be ensured through other options such as oral information, inspection of files, provisions of transcripts of relevant documents, printouts of the relevant information, a summary of the personal data in an intelligible form etc. When sending information to the data subject security should be ensured (secure email channels, physical mail, self-service tools).

Example 17: The right to access the video recording

The data subject requested a video recording of the screening test from the Finnish Police University College (controller). However, the controller refused to provide a copy because the video **showed other students participating in the exam**. Furthermore, according to the controller, it was technologically not possible to make a copy of the video recording that would only show the data subject. So instead, the controller provided the data subject with a written explanation of the test results and invited the data subject to view the video recording at the controller's facilities. The DPA held first that giving written information about the screening test results **does not release the controller from its obligation to provide a copy of the video recording**. In particular, the controller should consider applying technical measures such as video anonymisation to preserve the privacy of other persons. Consequently, the DPA ordered the controller to provide the data subject with a copy of the video recording.

When providing information to data subject the controller needs to make sure that rights and freedoms of others are not adversely affected (e.g. all information that potentially pertain to other persons should be deleted or blackened out).

The time limit to respond to a data subject's access request is without un**due delay or at least within one month** of the receipt of the request or within one month of receipt of any information requested to confirm the requester's identity. The time limit is calculated from the day of receipt of the request or other requested information (whether it is a working day or not) until the corresponding calendar date in the next month. If the case is complex or a large number of requests were received from the individual, the deadline can be extended for a further two months.

Right of rectification

Data subjects have the right to obtain without undue delay from the controller the **rectification of inaccurate personal data** concerning them and **the right to have incomplete data completed** (Article 16 GDPR). The right to rectification stems from the principle of accuracy.

Personal data are **incorrect** if the facts about the data subject set out therein do not objectively correspond to reality. The assessment of whether personal data are accurate and complete must be made in light of the purpose for which that data were collected. With respect to **incomplete data**, the

concept of completeness should be understood in relative terms as data sets are never complete. Certain data could be considered complete in one processing context, while the same data could be seen as incomplete in another. This also suggests that the right to rectification does not oblige controllers to rectify personal data when the inaccuracy is not relevant for the purposes of the processing.

Example 18: The German Federal Administrative court - registry error

A data subject born in Turkey but living in Germany had his date of birth first recorded in the civil status register in Turkey as 1 January 1956, this was later corrected to 1 January 1958. When the data subject moved to Germany first the 1958 birth date was entered in the register of residents. In 2015, the births date was changed in Turkey to 1 January 1953 and he was issued a new Turkish passport. This change of date was not, however, reflected in the official German registers and had an impact on the year he could receive his German pension. The German Federal Administrative Court decided that the data subject's request for rectification of his date of birth was unsuccessful as **the burden of proof** regarding the accuracy of the data designated to replace the currently processed data **lies on the data subject**. Since the data subject could ultimately not prove his actual date of birth, the Court decided in favour of the controller.

Right to erasure

Data subjects have the right to obtain from the controller **the erasure of personal** data concerning them without undue delay (Article 17 GDPR). Although some scholars have referred to the right of erasure as the most ambiguous right within the GDPR, as it is uncertain if data can ever be fully or properly erased, this right constitutes a very important safeguard for the enforcement of the data minimisation principle.

This right is **not absolute** and can only apply if: (i) data are no longer necessary; (ii) consent is withdrawn and no other legal basis exists; (iii) the data subject objects and there are no overriding legitimate grounds for processing; (iv) personal data were processed unlawfully; or (v) personal data have to be erased to comply with a legal obligation of the controller.

***The r*ight "to be forgotten"** or the right to request de-listing is similar but not the same as the right to erasure. It is a relatively new right which evolved from the case-law of the Court of Justice of the European Union (CJEU). Also, this right is not absolute as the source data might have to be retained for legal reasons or reason of public interest and the right only refers to the ease of access to information via search engines such as Google.

Example 19: The CJEU - Google Spain

Mario Costeja González did not pay his social security debts, and this was published in a local Spanish newspaper on the order of the Spanish Ministry of Labour and Social Affairs. Through the search engine Google, this news item appeared prominently every time someone searched his name. The CJEU held that an internet search engine operator is responsible for the processing that it carries out of personal information which appears on web pages published by third parties. Hence, it needs to consider requests from individuals to remove links to freely accessible web pages resulting from a search on their name.

Right to object

Data subjects can **object to the processing** on grounds relating to their particular situation, if the processing is based on public interest or legitimate interest, including profiling based on these provisions (Article 21 GDPR).

If the data subject objects, the controller shall no longer process the personal data, unless it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject or if processing is necessary for the exercise or defence of legal claims.

Example 20: The Dutch District Court of Midden-Nederland - balancing of interests

In a Dutch town a group of people was looking for paranormal activity at the grave of recently deceased children at a cemetery, with the permission of the director of the cemetery. The parents of the children learnt about it and asked the municipality to reveal the names, addresses and residences of these persons. The people holding the séance did not want their data to be given, as they had received serious threats as a consequence of the incident and they felt unsafe. Therefore, the paranormal group invoked their right to object. The mayor, after balancing the parents right to know the identity of the people and the right of the members of the paranormal activity to protection of their data, decided that the interest of the paranormal group is more important than the one of the parents of the deceased child. The Court held that **the safety aspect weighed heavily**. Although the interests of the parents were important, they did not outweigh the interests of the data subjects. Therefore, the Court ruled that the information requested should not be provided.

Right to restrict processing

*Data subjects have the right to obtain from the controller **restriction of processing** in four cases: (i) where they contest the accuracy of personal data; (ii) where the processing is unlawful: (iii) where data are required by the data subject for legal claims; and (iv) where the data subject has objected to processing (Article 18 GDPR). This right al*lows data subjects to temporarily limit the type of processing operations that a controller can perform on their personal data. During the restriction period the controller can only **passively store** the personal data.

Right to data portability

*Data subjects have **the right to receive the personal data** concerning them, which they have provided to the controller in a structured, commonly used, machine-readable format and **have the right to transmit these data** to another controller without hindrance from the controller to which the personal data have been provided (Article 20 GDPR and recital 68). The purpose of this new right is to empower data subjects and to rebalance the relationship between data subjects and controllers by giving data subjects control over their personal data.*

The right to data portability only applies if processing is based on consent or is necessary for the performance of a contract and the processing is carried out by automated means. It covers data provided knowingly and actively by the data subject as well as any data generated by a data subject's activity.

Rights related to automated processing and profiling

Data subjects have the **right not to be subject to a decision based solely on automated processing**, including profiling which produces legal effects concerning an individual or similarly significant affects for the individual (Article 22 GDPR) and the **right to explanation of decision-making logic** (algorithmic transparency).

Also, this right is not absolute and does not apply if: (i) the decision is necessary for entering into or performance of a contract; (ii) a data subject has explicitly consented; and (iii) the decision is authorised by EU or MS law. If a decision about an individual based on automated processing has a legal effect on an individual, such a data subject should have the right to obtain human intervention and to express his or her own point of view and contest the decision.

The right to data portability and the right not to be subject to automated individual decision-making are the rights which make the GDRP future-proof and ready for the digital age.

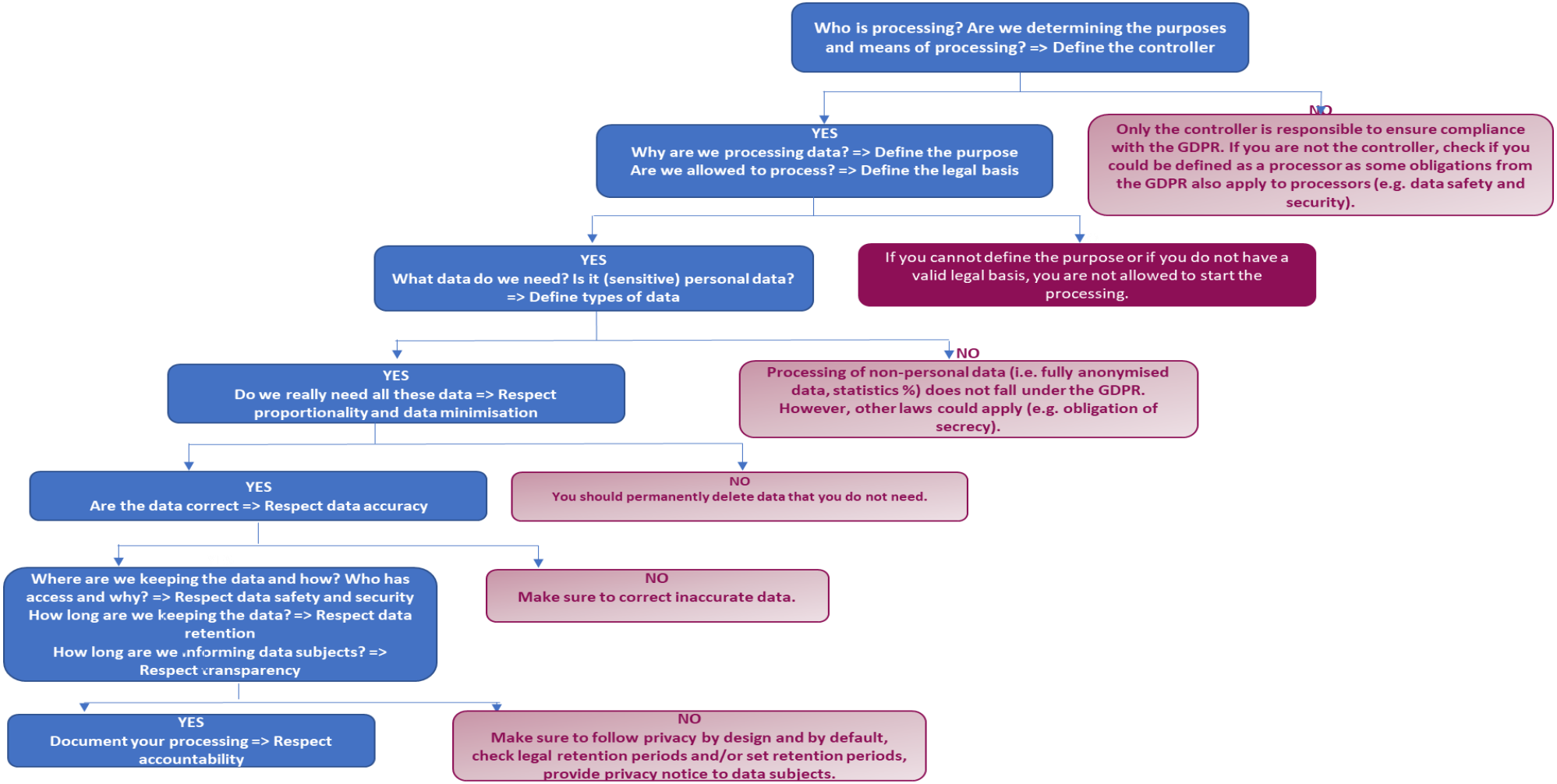
4.3 Restricting data subject rights

Under certain circumstances, the EU or MSs law may restrict the scope of the obligations and data subjects' rights (Article 23 GDPR). Any such **legislative measure** must respect the essence of the fundamental rights and freedoms and should be necessary and proportionate in a democratic society to safeguard qualified public interest.

Legal measures restricting data subjects' rights must contain specific provisions at least: on the purpose of the restrictions, their scope, the affected categories of personal data, safeguards, controller, storage periods and risks to the rights and freedoms of others.

5.0 Check list

Figure 3: Data processing check list



Annex I: Fictional case study

Facts of the case - purpose of processing and types of data

Due to a recent workplace accident resulting in 9 workers being wounded on a construction site in town X, the **Analysis and Intelligence Unit of the Labour Inspectorate** (affiliated with the Ministry for Labour) is **interested in the analysis of information related to the working time and remuneration** of some construction workers that are currently posted to their territory.

The Labour Inspectorate is interested in analysing some specific information that could **help the authority to tackle specific social dumping practices** (e.g. remuneration below applicable collective agreements) considering the following indicators:

- Sector of activity: 412.Construction of residential and non-residential buildings
- Geographical scope: specific region where the accident took place
- Companies with at least 40 workers currently posted when the data are retrieved
- Companies coming from other EU Member States operating simultaneously in 3 or more construction sites during the indicated period (October 2022)

For this purpose, a formal request has been made to the **Ministry for Social Protection** (owner of the database where such information is stored) to obtain the following information **in order to target companies at risk of no compliance**:

- Name and surname
- Sex
- ID number / passport number
- Date of birth
- Nationality
- Address
- Name and seat of the employer
- Party for whom the services are provided
- Location of work
- Period of posting (number of days)
- Remuneration / basic monthly salary (in EUR)
- Other monthly allowances (in EUR)
- Unemployment benefits received in 2022 (Y/N)
- Victim of an accident at work in 2022 (Y/N)

Questions to be answered

- *Who is the person responsible? Who is processing the data?*
- *Why is the Analysis and Intelligence Unit of the Labour Inspectorate seeking to process data? What is their purpose?*
- *Is the Labour Inspectorate allowed to process such data? What is the legal basis for processing?*
- *What data does the Analysis and Intelligence Unit need? Are all these data personal data?*
- *Does the Analysis and Intelligence Unit really need all the requested data? Could the same purpose be achieved with less data?*
- *Are the data correct and is there a way to check the accuracy of data? Does the Analysis and Intelligence Unit need all these data to ensure that they have a correct data set?*
- *How should the Analysis and Intelligence Unit inform data subjects about processing of their data?*

Facts of the case – data security

Ten days later, the Analysis and Intelligence Unit **received an email with one Excel file that was encrypted and could only be opened upon the submission of a password that came afterwards in a separate email**. Underlying documentation was stored on a **USB key** that was also sent to the Unit's headquarters. All documentation received included comprehensive information about 5 companies, including details about workers, that were selected using the indicators described above. Whilst all requested information had been received, **documentation also included other substantial and relevant information that could be useful for the Unit's work for other investigation purposes** (e.g. medical reports from a healthcare provider regarding some workers that sustained workplace accidents, copies of IDs).

In the course of its investigative analysis, the Analysis and Intelligence Unit has **extracted the information** from the received Excel file and documentation from the USB key **into 5 separate excel files**, one per each identified company. For each file, every separate tab includes information about an individual worker employed in the company (including images and pdfs). All these "clean" excel files have been **placed in a separate folder in the Unit's cloud**.

Questions to be answered

- *Where is the Analysis and Intelligence Unit keeping the data? How should it ensure the safety and security of data?*
- *How long should the Analysis and Intelligence Unit keep the data?*

Facts of the case – request for further information

The Analysis and Intelligence Unit is considering **sending formal notifications (summons)** to the main contracting undertakings that have contracted with the posting companies (and not directly to the companies that post workers as they are registered in another Member State) to provide the Inspectorate with further details related to the composition of remuneration, timeslips and payslips of all the identified workers. The Unit is not sure what information about individual workers they could share with the undertakings.

Questions to be answered

- *Can the Analysis and Intelligence Unit send to the undertakings individual Excel files in order for them to check the information and update it?*
- *Should the Unit rather include in the summons a limited amount of information identifying workers from these Excel files? Which information should they include in the summons?*

Facts of the case – transfer of data

At the same time, **the Health and Safety Unit** (another department in the Labour Inspectorate) is **interested in analysing this data** and has requested the Analysis and Intelligence Unit to forward all received documentation via an internal email so they can investigate any potential violations of occupational safety and health when it comes to accidents at work.

Questions to be answered

- *Can the Analysis and Intelligence Unit forward such data to the Health and Safety Unit in the same Labour Inspectorate?*

Annex II: Further reading

This section of references includes main legal documents as well as publications by EDPB, EDPS, and national DPAs as well as case law by the ECtHR, and CJEU. All sources of information are presented in an overview table which for every source presents information on the type of source, the topics covered and specifies the hyperlink. The list of further reading consists of three types of sources (guidelines, case law or national DPA decisions, and legislation).

Table 1: Further reading

Name	Type of Sources	URL	Topics
AEPD (Spanish DPA), Decision PS/00436/2021	Case law	https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS-00436-2021&mtc=today	Transparency – information notice
AEPD (Spanish DPA), Decision PS/00078/2021	Case law	https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00078/2021	Data minimisaton and proportionality
APD/GBA (Belgium DPA), Decision 147/2022	Case law	https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_147/2022&mtc=today	Data minimisaton and proportionality
BVerwG (the German Federal Administrative Court), Case 6 C 7.20	Case law	https://gdprhub.eu/index.php?title=BVerwG_-_6_C_7.20&mtc=today	Right to rectification
Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)	Legislation	https://www.coe.int/en/web/data-protection/convention108-and-protocol	International data protection

Datatilsynet (Danish Data Protection Agency), Guidance on the use of cloud	Guidelines	https://www.datatilsynet.dk/Media/637824108733754794/Guidance%20on%20the%20use%20of%20cloud.pdf	Cloud computing
Digi Távközlési és Szolgáltató Kft. V Nemzeti Adatvédelmi és Információszabadság Hatóság, C-7/21	Case law	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0077	Principle of purpose limitation
Directive (EU) 2016/680 – Law Enforcement Directive (LED)	Case law	https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680	Processing of personal data by competent authorities for law enforcement purposes
EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR	Guidelines	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en	Controller and processor
EDPB, Guidelines 05/2020 on consent under Regulation 2016/679	Guidelines	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en	Consent as a legal basis
EDPB, Guidelines 02/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the	Guidelines	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-	Contract as a legal basis

provision of online services to data subjects		under-article-61b_en	
EU Charter of Fundamental Rights	Legislation	https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en	Right to the protection of personal data
European Convention on Human Rights (ECHR)	Legislation	https://www.echr.coe.int/documents/convention_eng.pdf	Right to privacy
Google Spain and Google, C-131/12	Case law	https://curia.europa.eu/juris/liste.jsf?num=C-131/12	Right to be forgotten
Jehovan todistajat, C-25/17	Case law	https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-25/17	Joint controllership
Patrick Breyer v Germany, C-582/14	Case law	https://curia.europa.eu/juris/liste.jsf?num=C-582/14	Broad definition of personal data
Peter Nowak v Data Protection Commissioner, Ireland, C-434/16	Case law	https://curia.europa.eu/juris/liste.jsf?num=C-434/16	Definition of personal data
Rb. Midden-Nederland (the Dutch District Court of Midden-Nederland), case C/16/542054 / KG ZA 22-341	Case law	https://gdprhub.eu/index.php?title=Rb._Midden-Nederland_-_C/16/542054_/_KG_ZA_22-341&mtc=today	Right to object

Regulation (EU) 2018/1725	Legislation	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725	Processing of personal data by EU institutions and bodies
Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR)	Legislation	https://eur-lex.europa.eu/eli/reg/2016/679/oj	Text of the GDPR
Tietosuojavaltuutetun toimisto (Finnish DPA), Decision 1788/152/22	Case law	https://gdprhub.eu/index.php?title=Tietosuojavaltuutetun_toimisto_(Finland)_-_1788/152/22&mtc=today	Right of access
WP29, Guidelines on Consent under Regulation 2016/679	Guidelines	https://ec.europa.eu/newsroom/article29/items/623051/en	Consent
WP29, Guidelines on the right to "data portability"	Guidelines	https://ec.europa.eu/newsroom/article29/items/611233/en	Right to data portability
WP29, Guidelines on Data Protection Officers ('DPOs')	Guidelines	https://ec.europa.eu/newsroom/article29/items/612048	Data Protection Officer
WP29, Guidelines on transparency under Regulation 2016/679	Guidelines	https://ec.europa.eu/newsroom/article29/items/622227/en	Transparency
WP29, Opinion 04/2007 on the concept of personal data	Guidelines	https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf	Definition of personal data

WP29, Opinion 03/2010 on the principle of accountability	Guidelines	https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf	Principle of accountability
WP29, Opinion 03/2013 on purpose limitation	Guidelines	https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf	Principle of purpose limitation