Regulatory Analysis
Deliverable D2.2

Editor
Francesca Gaudino, Davide Cascone (BAK)

Reviewers
Georgios V. Lioudakis (ICT abovo)
Spiros Alexakis (CAS)

Date
31/10/2018
Classification
Public

Contributing Author

Name	Partner
Davide Cascone	BAK

Version History

#	Description
1	First version (19/10/2018)
2	Internal review version (26/10/2018)
3	Internal review comments (27/10/2018)
5	Final version (29/10/2018)

Table of Contents

1 Introduction

This deliverable aims to give an overview of the main issues around the European data protection legislation as the General Data Protection Regulation (hereinafter "GDPR")[1] came into force on 25th May 2018. GDPR, indeed, has affected the data protection theme under a wider perspective not only in terms of geographical application, but also the higher level of awareness generated among the operators while processing personal data.

More specifically, data protection should not be considered as the mere "*right to be let alone*"[2] anymore. Given the fluidity of the digital environment affecting all the sides of private life, the actual meaning of data protection consists not only in the sole commitment of the individual to understand how his data are processed, but also the duty in charge of any data controllers to ensure they carry out processing of personal data through adequate means and in compliance with law[3].

As a result, the legal framework aims to have common requirements for a geographical scope of application that needs to get wider and wider, taking into account the significant degree of connectivity, self-expression and scope for delivering value to organisations and consumers given by the internet and the digital market[4]. The goals here are either raising the level of awareness of privacy issues and encouraging citizens of having more control over the information they provide online.

These are the reasons why the three main EU institutions —European Parliament, Council and European Commission— started the negotiations and discussion on replacing the Directive 95/46/EC[5] on data protection with a regulation. The work of the EU institutions was also quickened by the leading case *Maximilian Schrems v. Data Protection Commissioner*[6] of 6th October 2015 that have criticized the legal basis on which all U.S. companies relied for the management of EU citizens personal data while being transferred to the United States jurisdiction, the *Safe Harbour*. This leaded to the adoption of a new legal framework, the *E.U. - U.S. Privacy Shield*, for the transfer of personal data from EU jurisdiction to U.S. and also raised the attention of the public opinion upon the data protection.

The General Data Protection Regulation ("GDPR")[7] entered into force on 25th May 2018, after two years since its publication, giving organizations and data protection authorities a limited window to get prepared for understanding and complying with the new issues and requirements. Being regulation, the GDPR is directly applicable to all EU Member States laws, creating unique legislative framework and reshaping the way organizations across the region approach data privacy for EU residents. The main point of reference the

[1] 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.
[2] See S. Warren and L. Brandeis, *The Right to be Let Alone*, Harvard Law Review, 1890, vol. 4, n. 5.
[3] See also the *Charter of Fundamental Rights of the European Union* (2000/C 364/01), art. 8.
[4] See S. Rodotà, *Il mondo della rete. Quali i diritti, quali i vincoli*, Laterza, 2014.
[5] 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.
[6] CJEU, case C-362/14.
[7] 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.

context of the digital economy, whose constant growth affects the way data is collected, stored and used, as well as individuals perceived the role played by the information in the global market.

2 Scope of application

2.1 Geographical scope of application

The territorial application of the Regulation depends on the joint application of a set of criteria which are not only geographical, but also logical and connected with the destination of the activities carried out by the data controller and the data processor.

In essence, the GDPR has extended the scope of application to the processing of personal data carried out by data controller or data processor (the definition of these roles shall be analysed later in chapter 4) in the context of an establishment inside —but also outside— the European Union, provided that a preliminary analysis is conducted on the basis of some key factors. Such criteria are affected by the characteristics of the data processing, the data controller and data processor, where the establishment of the controller/processor is located and who are the data subjects involved, and are the following: (i) geographical location of the establishment; (ii) consistency between business activities and data processing operations at stake, and (iii) where the data subjects are based while their personal information are processed.

Explaining the criteria above, it is worth to underline that the term establishment is not necessary identified as the registered office of the organisation[8]. According to recital 22 of the GDPR, the legal form of the establishment is not a determining factor, whereas what matters is the "*effective and real exercise of activity through stable arrangements*". In evaluating this, it is crucial to understand where the services and the activities of the data controller in respect of that processing are mainly or entirely directed at, since the data protection law would apply even to the data controller operating —even if minimally— through stable arrangements in the territory of a different Member State than the one where he is legally registered. This is a crucial factor to calculate the effective degree of stability of the arrangement through which the data controller carries out data processing operations[9].

At the same time, the establishment always requires human organization managing the arrangements. As remarked in the opinion 8/2010 of the Art. 29 Working Group[10], a stable arrangement does require both human and technical resources necessary for the provision of services. A server or a computer is not likely to qualify as an establishment as it is simply a technical facility or mean for the mere processing of information[11].

It is a fact that the GDPR has a wider point of view, since it is directed to the EU jurisdiction as a whole. However, the reasoning must still rely on the principles set forth in the CJEU's decision *Weltimmo*, even though the connection is not restricted to a specific Member State territory, but it is extended to the entire Union, which is considered as a unique and bigger entity. What matters now it is getting whether the data controller carries out its activities directing to the European Union, regardless of the differences among Member States. Of course, this may involve difficulties to redefine the concept of establishment created by CJEU rulings before the GDPR came into force, evaluating if there would be consequences even for data subjects that are not based in the Member State where the data controller effectively directs its activities.

[8] CJEU, *Weltimmo*, C-230/14, par. 66(1).
[9] *Ibidem*, par. 31: "*it should be considered that the concept of 'establishment' […] extends to any real and effective activity - even a minimal one - exercised through stable arrangements*".
[10] WP29, *op. 8/2010*, pag. 14.
[11] *Ibidem*, pag. 12.

Therefore, the GDPR has kept the reference to the establishment strictly related to the "context of activities" carried out by the data controller or the data processor, as already underlined by Directive 95/46/EC. As a result, pursuant to art. 3(1) GDPR, the application of the law depends on the link between the t based in the Union and the processing activity. Indeed, the notion of context of activities implies that the applicable law is the law of where an establishment of the controller or processor is involved in activities relating to data processing[12]. To this purpose, it is important to verify the degree of involvement to the processing operations as well as the nature of the processing, since if an establishment processes personal data in the context of activities of another establishment based in the EU, then the GDPR may apply. That is why, for instance, a company centralises personal data of the employees from all its subsidiaries or braches in one single database located in a third country (e.g. United States), not only the data protection law of the third country, but also the GDPR will apply.

A third element affecting the territorial application of the Regulation is the location of the data processing. More precisely, the GDPR applies to the data processing regardless of whether it takes place in the Union or not[13]. This means that the geographic identification of where the data processing is carried out does not matter while defining the applicability of the Regulation.

On the other hand, two are the crucial factors to determine the applicability of the GDPR to data processing activities carried out by data controllers or processors outside the Union: (i) to clarify whether data subjects "are" in the European Union and (ii) the categories of processing activities. Therefore, the reasoning must not rely on the nationality or the residence of individuals involved (as mentioned in recitals 2 and 14 of the GDPR), but on their sole presence in the EU territory[14]. However, if this enlarge the scope of application, it also makes it more difficult to determine, with particular regard to individuals who are going through EU for a limited period of time (e.g. tourists).

Moreover, art. 3(2) GDPR identifies two macro-categories of processing activities where the Regulation may apply. These are the following:

a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union
b. the monitoring of data subjects' behaviour as far as their behaviour takes place within the Union.

As per point a. it should be ascertained whether it is apparent that the controller or processor envisages offering goods or services to data subjects in one or more Member States in the Union. Such intention may arise whenever it is used a language or a currency generally used in the EU State involved with the possibility of ordering goods and services in that other language, or if customers or users in the Union are mentioned. Instead, the acceptance of the offer by the data subjects is not a determining factor, as well as the State where any possible joint controllers are based. For instance, even the provider of social networking services should understand that the processing of personal data of third parties (e.g. photography) who are in the Union from

[12] *Ibidem*, pag. 13.
[13] See art. 3(1) GDPR.
[14] The reference to the residence within the EU was dismissed during the preparatory work after the initial proposal.

users who are outside the Union makes the GDPR applicable and such third parties are data subjects, consequently[15].

The monitoring activity in point b. only relates to the behaviour of data subjects taking place within the Union. To this purpose, recital 24 of the GDPR says that it should be ascertained whether the natural persons are tracked on the internet involving, for instance, the use of profiling techniques, in order to make a selection and make any relevant analysis concerning the personal preferences, behaviours and attitudes[16]. The former Article 29 Working Party[17]has provided some indications of what represents a monitoring activities. Among others, online behavioural based advertising; location tracking by mobile apps; or monitoring of fitness and health data through wearable devices[18]. In this list we also have connected devices, such as smart cars or home automation, witnessing how the *Internet of Things* ("IoT") increasingly contributes in profiling our habits.

2.2 Material scope of application

Pursuant to art. of the 2 GDPR: "*This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*". The **processing** of **personal data** has remained as the main focus of data protection legal framework, that was already defined by the Directive 95/46/EC.

Art. 4(1) defines personal data as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

Art. 4(2) defines processing as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

At first it is clear is that the Regulation, following the approach of the former Directive, has adopted broad definitions of what is a personal data, that is, in essence, anything which makes one individual identified or identifiable at least. As to the term processing, in practice, any kind of activity that is performed on personal data represents data processing, even the mere consultation of personal data or the network monitoring.

[15] See recital 23: "[…] *factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union*".
[16] See recital 24: "[…] *In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*".
[17] Article 29 Working Party was an advisory board established by Directive 95/46/EC on the protection of personal data and now replaced by the European Data Protection Board.
[18] See WP 243, *Guidelines on data protection officers*, 2016.

That being said, the wording of art. 2(1) GDPR restrains from the scope of application the processing of personal data wholly by manual means and without the support of a structures filing system. Therefore, files as well as their cover pages, which are not structured should not fall within the scope of the GDPR[19].

At the same time, to determine whether a natural person is actually identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by another person, taking into consideration factors like the available technology at the time of the processing. The data protection legal framework should therefore not apply to anonymous information, which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. It turns out that this Regulation does not concern the processing of anonymous information, such as the collection of anonymous data for statistical or research purposes, as they cannot be considered as personal data[20].

Another implicit exception to the material scope of application of the GDPR is the processing of personal data of deceased persons[21], given the fact that data is no more personal when the link with a living human being disappears. However, the GDPR leaves to the national legislation the chance to face such a topic. For instance, the latest Italian Legislative Decree n. 101/2018 (but also the former Privacy Code) regulates this issue by admitting that any person acting for his/her own interest or on behalf of the deceased person, even for family-related reasons may exercise the rights regulated under art. 15 et seq. of the GDPR.

Art. 2(2) of the Regulation insists on the describing the limitation to the material scope of application through the following sectors:

(a) *in the course of an activity which falls outside the scope of Union law*. This provision must be read in connection with recital 16), where it is underlined that any activity falling outside the EU law cannot be regulated by the GDPR. This does not mean that such issues cannot be regulated by the national legislator, since one of the most important principle of the EU law is the subsidiarity, so that whichever matter is not addressed by the Union, the competence is upon Member States[22]. In particular, activities concerning national security, that should refer to intelligence operations and any other field affecting the protection of the national interest, as a more accurate definition of 'national security' from EU legislation and case-laws is still missing.

(b) *by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU*. This restriction applies to EU policies concerning common foreign and security policy, that are decided and coordinated by the EU High Representative of the Union for Foreign Affair and Security Policy.

(c) *by a natural person in the course of a purely personal or household activity* regardless of the presence of gainful interest or whether activities are carried out in the digital context[23].

(d) *by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention*

[19] See recital 15 GDPR.
[20] See recital 26 GDPR.
[21] See recital 27 GDPR.
[22] Art. 4 TEU.
[23] See recital 18 GDPR.

of threats to public security. This area is covered by another EU legal mean, that is EU Directive 2016/680 applying on the processing of personal data and their free movement among competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[24].

[24] See *Directive (EU) 2016/680* 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

3 Definition of personal data and data processing

3.1 Personal data

The definition used in art. 4(1) GDPR substantially recalls what already identified by the Directive[25], providing a broad definition[26] and focusing on the link to an identified or identifiable individual. Personal data are therefore related to natural person only.

Art. 29 WP in its Opinion issued on June 2007[27] expressly states the following with regard to the wide scope of the definition of personal data under the former Directive: "It needs to be noted that this definition reflects the intention of the European lawmaker for a wide notion of "personal data", maintained throughout the legislative process. The Commission's original proposal explained that "*as in Convention 108, a broad definition is adopted in order to cover all information which may be linked to an individual*"[28]. The Commission's modified proposal noted that "*the amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual*"[29], a wish that also the Council took into account in the common position[30]".

To have a deeper comprehension of the characteristic of personal data, we must consider four different elements: (i) information, (ii) natural person, (iii) link, and (iv) Identification/Identifiability.

As far as the information is concerned, what matters is the nature of the information, since the concept of personal data includes any objective and subjective statements about a person[31] regardless it is proven or not, such as an audio file, an image or contact details. The content or the format of the information is not crucial as well. Personal data includes data providing any sort of information touching the individual's private life, but also information regarding whatever types of activity is undertaken by the individual, like that concerning working relations or the economic or social behaviour of the individual. Also, any form is acceptable in identifying personal data, such as alphabetical, numerical, graphical, photographical or acoustic. It includes information kept on paper, as well as information stored in a computer memory by means of binary code, or on a videotape, for instance. It follows that automatic processing of personal data is covered within its scope.

The discipline of the GDPR applies to natural persons, that is, to human beings. The right to the protection of personal data is, in that sense, a universal one that is not restricted to national or regional borders. Another aspect of this point refers to the fact that the Regulation intends personal data as referring to living individuals, so that deceased persons are not included in the scope of application of the GDPR.

---

[25] See art. 2, lett. a) Directive: *"personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*.

[26] See the definition mentioned at pag. 9.

[27] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[28] COM (90) 314 final, 13.9.1990, p. 19 (commentary on Article 2).

[29] COM (92) 422 final, 28.10.1992, p. 10 (commentary on Article 2).

[30] Common position (EC) No 1/95, adopted by the Council on 20 February 1995, OJ NO C 93 of 13.4.1995, pag. 20.

[31] See WP Opinion 4/2007 on the concept of personal data.

However, recital 27 clearly states that Member States may provide for rules on this matter, as already recalled by the CJEU[32]. For instance, the Italian Legislative Decree 101/2018[33] harmonizing the GDPR provisions with the Italian privacy law extends the scope of application of data protection law and admits the exercise of privacy rights concerning data of deceased persons by individuals having their own interest or acting as representative, or due to a family link.

Moreover, certain data protection rules may still indirectly apply to information relating to businesses or to legal persons, in a number of circumstances, even though the material scope of application of the GDPR refers only to natural persons. For example, some provisions of the E-privacy Directive 2002/58/EC extend to legal persons. Article 1 thereof provides that "2. The provisions of this Directive particularise and complement the GDPR for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons." Accordingly, Articles 12 and 13 extend the application of some provisions concerning directories of subscribers and unsolicited communication also to legal persons[34].

Third key factor is the relation —the link— between the information and the individual, which makes him identified or identifiable. This relationship may be characterized by the presence of a content, purpose or result element.

1. The "content element" means that the content of information itself relates to a data subject, that the content of the information itself is about a data subject, for example the information on a company's client that is contained in the client's folder is an information that relates to that client from the content element perspective.
2. The "purpose element" is present when an information is meant to be used with the purpose of evaluating, treating, or influencing in a certain way the status or the behaviour of a data subject.

Article 29 Data Protection Working Party gives as an example the call log of a telephone inside a company office, which may give information about the calls made, which may be information about the company (considered as the contracting party of the telephone operator), about the employee that has been granted the telephone by the company (the telephone is supposed to be controlled by the employee and calls are therefore supposed to be made by him), and also about the data subjects called by that telephone. It follows that the same information (call logs) may be related to different data subjects according to the different purposes for which said information is collected and processed.

3. The "result element" means that data relate to a data subject when their use is likely to have an impact on the data subject's right and interests, being it understood that said impact does not necessarily need to be significant.

The content, purpose and results elements are alternative and not cumulative conditions, which means that the presence of only one of them is enough to qualify an information as relating to a certain data subject.

Coming to the last crucial factor, it is noted that the reported definition splits the category of personal data in two sub-categories: personal data that identify directly the data subject[35], so-called identification data; and

[32] Judgment of the European Court of Justice C-101/2001 of 06/11/2003 (Lindqvist), par. 98.
[33] See art. 2-*terdecies* Legislative Decree 101 of August 10th 2018.
[34] To this purpose, see art. 122 et seq. of the Italian Privacy Code (Legislative Decree 196/2003).
[35] The data subject is the subject whose data are processed.

personal data allowing an indirect identification of the data subject. This is strictly connected with the content of recital 26 GDPR, where it is said that "*to determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by any other person to identify the natural person directly or indirectly*".

Identification data are basically pieces of information that distinguish a data subject from all the others and therefore act as identifying factors. With this regard, "*the name of the person is indeed the most common identifier, and, in practice, the notion of "identified person" implies most often a reference to the person's name*[36]".

In contrast, indirect identification data are data that do not identify directly the data subject, yet they may identify the data subject through association with other available information, thus in an indirect way. It seems appropriate recalling that the wording "other information available" has regards not only to other information available to the controller[37], namely the entity primarily in charge of the data processing, but also to any information that may be possessed by any third party other than the controller. It is important to focus on the circumstance that the definition of indirect identification data is significantly extended by the circumstance that the identification of the data subject may be possible by reverting to any information possessed by any third party other than the controller.

Article 29 Data Protection Working Party clarified the foregoing matters on direct and indirect identification through the examples of electronic processing of data. When a computerized file stores personal data, it normally generates a unique identifier for the entries registered that is the data subjects that are registered, in order to prevent confusion between the different registrations. On the web, the device deployed for traffic surveillance allow to define and identify in an easy way the behaviour of a certain machine, and since the machine is operated by a data subject (user), ultimately the behaviour of said user. It follows that the name as such loses its importance in the process of identifying a data subject, and may no longer be required for identifying purposes, and the definition of personal data mirrors this standpoint[38].

With regards to dynamic IP addresses, Art. 29 Working Party considers them as personal data in the sense of information that relates to an identifiable data subject. In a Working Document adopted in the year of 2000 in relation to the issue of Privacy on the Internet[39], Art. 29 Working Party has taken the view that "*Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically "log" in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases, there is no doubt about the fact that one can talk about personal*

[36] See WP Opinion 4/2007 on the concept of personal data, pag. 13.
[37] *The controller under Article 1, letter d) of the GDPR is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".*
[38] Report on the application of data protection principles to the worldwide telecommunication networks, by Mr. Yves POULLET and his team, for the Council of Europe's T-PD Committee, point 2.3.1, T-PD (2004) 04 final.
[39] Working Document WP 37: Privacy on the Internet - An integrated EU Approach to On-line Data Protection, adopted on November 21, 2000, and available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf.

data in the sense of Article 2 a) of the Directive …)" (Reference is made to the former Data Protection Directive).

As a further explanation of the meaning of indirect identification data, it seems appropriate to recall a Decision of the Italian Data Protection Authority (the "Garante") issued on January 9, 1999 in relation to the publication on a scientific journal of the radiography of a woman. The x-ray photograph was displayed with reference to only the first name and the age of the woman. The Italian Data Protection Authority held that such information is personal data, namely a quasi-anonymous data, because considering the peculiar name of the woman, the age of the woman, the circumstance that the woman lived in a small town where basically anyone might have known the other people from the same town, and the means of diffusion of the information (notably publication on a scientific journal), the woman might have been identified by someone, especially by other people form the same town of the woman[40].

It should also be clarified that the action of identifying the data subject is not necessary as such, it is enough that in general terms said identification is possible, notwithstanding the fact that the relevant data controller is willing to proceed to the identification or not. In brief, the potentiality of identification makes the data falling within the definition of 'personal data' and as such they are subject to the applicable data protection legislation, irrespective of the intention of the controller that holds and processes said data.

3.2 Special categories of data and "judicial data"

The GDPR (art. 9) identifies special categories of data, that include "[…] *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*". These are intended as the former "sensitive data" as described in Directive 95/46/EC[41] which deserve an stronger level of protection because of the higher risk for the rights and freedoms of the individuals if any infringements occur.

Therefore, the legal framework needs to provide the individuals with wider and stronger means to control the use and the destination of their personal information, but also to lower the level of risk in case of breaches. That is why the GDPR restricts the lawful processing of these data: "*such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*"[42].

Special categories of data are the following:

- *data revealing racial or ethnic origin:* this expression is only used to protect the individual subject to such a classification, whereby the use of the term 'racial origin' in this Regulation does not imply an

[40] The Decision of the Italian Data Protection Authority is published on the Bulletin n. 7 of January 1999, pag. 35, and available in Italian language at the following web address: http://www.garanteprivacy.it/garante/doc.jsp?ID=31031.
[41] This group of data had already been drafted by the ECHR Convention 108/1981.
[42] See recital 51 GDPR.

acceptance by the Union of theories which attempt to determine the existence of separate human races[43];

- *political opinions, religious or philosophical beliefs;*
- *trade union membership*, which is highly important in the field of employment and social security management;
- *biometric data*, referring to biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability[44]. The identification of individual is therefore carried out by comparing biometric data of an individual to a number of biometric templates stored in a database (i.e. *one-to-many* matching process), whereas the verification of an individual is made by comparing his biometric data to a single biometric template (i.e. *one-to-one* matching process);
- *health data,* which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services. A specific category of health data is *genetic data*, which are collected from biological samples and refers to genetic characteristic, related to their family background;
- *sexual life or sexual orientation.*

With particular regard to images, the Regulation says that "*the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person*".

The processing of these special categories of data is restricted, as the GDPR provides for a general prohibition with some determined exceptions, described in art. 9(2) GDPR. As a general rule, the processing of these data relies on the consent of data subjects, but it may be legitimated also in the following cases, alternatively:

- carry out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a Collective Bargain Agreement ("CBA") pursuant to Member State law;
- protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- the legitimate activities of a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- personal data which are manifestly made public by the data subject;
- whether the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

[43] See recital 51 GDPR.
[44] See WP193, Opinion 3/2012 on developments in biometric technologies.

- a substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;
- reasons of public interest in the area of public health, 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;
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Judicial data, instead, are meant as relating to criminal convictions and offences or related security measures. Their processing is limited to (i) when it is carried out relying on the control of official authority or (ii) when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Anyhow, the GDPR opens to Member States additional provisions on this issue, with special regard to the field of employment and social security. For instance, the Italian legal framework admits the processing of judicial data also on the basis of CBAs' clauses (i.e. the CBA of banking and finance area).

3.3 Data anonymisation and pseudonymisation

Having specified the meanings of personal data (in the sense of data that identify the data subjects both indirectly and indirectly) and that of data processing, it is left to determine what are anonymous data, meant as data rendered in such a way that the data subject is no longer identifiable. Thus anonymous data are data that do not allow, not even indirectly, the identification of the data subject.

Recital 26 of the GDPR, referring to anonymous data, says that "*the principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes*"[45]. This means that anonymous data fall outside the application of the GDPR, since they have characteristic which are way different from personal data *stricto sensu*: whenever the situation overcome the edge of identifiability by not having any type of link with a certain natural person, it means that data has lost any qualities rendering it personal data. Not being useful to identify the data subject, it falls outside the concept of personal data.

Again, the assessment of whether the data allow identification of an individual, and whether the information can be considered as anonymous or not depends on the circumstances, and a case-by-case analysis should be carried out with particular reference to the extent that the means are likely reasonably to be used for

[45] See recital 26 GDPR.

identification as described in Recital 26. This is particularly relevant in the case of statistical information, where despite the fact that the information may be presented as aggregated data, the original sample is not sufficiently large and other pieces of information may enable the identification of individuals.

In the above-mentioned Opinion, Art. 29 WP[46] defines anonymous data as: "any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, *taking account of all the means likely reasonably to be used either by the controller or by any other person* to identify that individual". Anonymised data "would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible".

In practice, data usually are not born as anonymous data, yet they are rendered anonymous through processing and elaboration activities (for example, elaboration in aggregate form). The result of said elaboration is aggregate data, but for the activities consisting in the first gathering and in the elaboration, data have been processed in the form of personal data, and thus they should be processed according to the applicable data protection legislation until they are made anonymous.

From the considerations outlined in this deliverable, it stems that the EU data protection legislation does not apply to anonymous data, and to data that do not fall within the definition of 'personal data' as set forth in the GDPR, for example when the data do not refer to natural persons, or when the data subject is not considered to be identified or identifiable.

However, the circumstance that the GDPR is not applicable, does not automatically preclude any kind of protection for the data subjects.

First of all, in implementing the GDPR the EU member states are granted a certain degree of freedom and flexibility, so they can extend the scope of application of the relevant national data protection legislation, as long as they do not breach other provisions of Community laws, and this concept has been clearly approved by the European Court of Justice[47]. For example, as outlined before, in some EU member states the national data protection legislation, differently from the GDPR applies not only to natural persons but also to legal entities. The same difference in approach may be taken with regard to matters like pseudonymised or key-coded data.

Pseudonymised and key-coded data represent personal data that are processed so that they become quasi-anonymous data. According to art. 4(5) GDPR, "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person[48].

In practice, they are data that usually provide the possibility to identify the data subject, an in this sense they are personal data to which the GDPR is applicable, but for these specific kinds of data the identification of the data subject is rendered more difficult by the data controller itself after collection of the data by disguising the

[46] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf
[47] Judgment of the European Court of Justice C-101/2001 of 06.11.2003 (Lindqvist), par. 98.
[48] This is a *privacy enhancing* technique, thanks to which the information related to the processing and able to make the data subject identifiable are kept separately.

identity of the data subject, which usually consists in the identification factors such as name and surname (for natural persons).

The reasons why the data controller renders the identity of the data subject not known at first glance should be retrieved in Article 5 of the GDPR[49], which sets forth the main principles for a lawful data processing, including the data quality principles, which may be regarded as representing a sort of benchmark of the all data protection legislation in the sense that the specific rules that discipline the data processing activity contained in the EU data protection legislation stem from these fundamental principles.

These principles are linked one with the others, and as to data quality, they provide that a data controller should collect and process only the kind and number of data that are functional and necessary to the specific processing purpose that is pursued.

Moreover, data should be kept in a form that identifies the data subject only when and as long as the identification is necessary for the processing purposes to be achieved. It follows that using pseudonymised and key-coded data instead of personal data that identify directly and immediately the data subject represents an adequate and necessary measure to protect data. It may for example be the case that data are necessary not in relation to the data subject to which they refer to, but in relation to their content, or other elements that may be retrieved from the data and that do not have connection with the identity of the data subject. It means that pseudonymisation falls within the technical and organizational measures required by the Regulation to protect data subjects' rights by lowering risks for data security and identifiability of individuals ("*singling out*")[50].

In conclusion, pseudonymised data that are retraceable are subject to application of the GDPR and disguise the identity of the data subject, which remains indirectly identifiable, so that they allow to backtrack to the data subject, yet the reidentification process may be performed only by certain subjects and only under predefined circumstances. For instance, when data subjects are included within clusters of data, pseudonymisation is the best way to maintain a low risk level while ensuring the identifiability of individuals and the possibility to understand the procedures that leaded to the target identification. This is usually carried

[49] Article 5 of the GDPR reads as follows: "*Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; 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 ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*".

[50] Recital 28 GDPR.

out by assigning a small group o people the access to certain information which are fundamental for the identification within the cluster.

Art. 29 WP in the aforementioned document on the concept of personal data[51] defines the pseudonymisation as the "*process of disguising identities. The aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity. This is particularly relevant in the context of research and statistics.*".

A personal data may be pseudonymised in a twofold way, that is in a way that allows and in a way that does not allow reidentification of the data subject.

Reidentification of the data subject is possible for example with the deployment of lists that map and match the real identities of the data subjects with the assigned pseudonyms or through use of two-way cryptography algorithms. In contrast, if the reidentification of the data subject is no longer possible after pseudonymisation, for example when one-way cryptography solutions are deployed, anonymised data are created.

The features of the pseudonymisation procedure as to results and effectiveness vary on the basis of different factors, for example the moment when it is deployed, the level of security against reverse tracing, the numbers of data subjects involved in the whole data processing, the technical possibility of associating other individually identified information relating to the data subject, etc.

In order to enhance the level of security and to provide a higher degree of protection to the identity of the data subject, the process of pseudonymisation should take place in a random and unpredictable way, and the number of pseudonyms deployed should be large enough to avoid re-using of the same pseudonym (one pseudonym should be used only once). Moreover, for a higher security degree, *the set of potential pseudonyms must be at least equal to the range of values of secure cryptographic hash functions*[52].

One important example of pseudonymisation is the use of key-coded data. The procedure that applies in relation to key coded data is that data and information pertaining to a certain data subject are earmarked by a code, and there is another specific document containing the key that associates the assigned codes with the identifying elements of the data subject (for example name, surname, date of birth, contact details such as address and place of residence), which is kept separately form the documentation containing the information referring to the data subject whose identity is disguised under the assigned code.

With regard to the issue of considering key-coded data as personal data under the GDPR, Art. 29 WP[53] makes two examples to clarify this issue, notably the examples of non-aggregate data to be used for statistical purposes and the key-coded data usually deployed for clinical trials.

The basic principle set forth by Art. 29 WP is that in order to assess if the key-coded data are personal data, focus has to be devoted to the question whether the data subjects may be identified starting from the key-

[51] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.
[52] Please refer to the Working document entitled "*Privacy-enhancing technologies*" issued by the Working Group on "privacy enhancing technologies" of the Committee on "*Technical and organisational aspects of data protection*" of the German Federal and State Data Protection Commissioners (October 1997), available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm.
[53] Please see above footnote.

coded data "*taking into account all the means likely reasonably to be used by the controller or any other person*". As to statistic activities, Art. 29 WP highlights that the use of unique codes as identifiers (meaning that the same code is not assigned to more than one data subject) increases the risk of identification since identification may indeed occur each time that it is possible to access the document or the key containing the correspondence between codes and data subjects.

In said case, consideration should be devoted to the risks of malicious intruders that gain access to said key, for example an external hack, someone within the data controller's organization that may unlawfully get access to said key or communicate it to unauthorized third parties, also in breach of professional secrecy and confidentiality obligations.

The risks above outlined, that may exist in practice notwithstanding the security measures adopted by the relevant data controller, make the key-coded data falling within the definition of 'personal data' under the GDPR.

In contrast, the above outlined risk is limited in case of deployment of codes that are not unique, in the sense that the same code may be assigned to different data subjects that are part of the statistic activities; for example the same code may be assigned to data subjects residing in different cities, and the same codes may be used for different years of the statistic surveys, and in such a case the possibility of identifying the data subject sharply decreases since for identification it would be necessary to access the key document and also to know the relevant year and city of residence of the data subject. In case this further information is no more available in any way, and it is not likely reasonably to be retrieved, the key-coded data may be considered as not referring to identifiable data subjects and therefore they would not be subject to the GDPR.

Going to analysing the case of data collected and used in the area of clinical trials with medicines[54], Art. 29 WP in the aforementioned document on the concept of personal data[55] recognizes that key-coded data are commonly used for said purposes.

The personal data on patients taking part to clinical trials are collected in data collection forms in which patients are usually identified by a code. The medical professional/researcher (usually referred to as the principal investigator) that is in charge of the clinical trial holds the document containing the 'key' to know the associations between the codes assigned and the identifiers elements of the patients, such as name and surname of the patients.

The so named sponsor, that is the pharmaceutical company that manages the clinical trials, together with or other third parties possibly involved in the clinical trials, only get the key-coded data, and usually do not have access to the identifying personal data of patients, since they are not interested in these data for purposes of the clinical trials: they are indeed only interested in the results of the trials.

The reason why there must exist a document through which it is possible to retrieve the real identity of patients is that in case of adverse effects or risks deriving from the medicines under trail, the principal

[54] The regulation on clinical trials with medicines is laid down by Directive 2001/20 of 4 April 2001 on the implementation of good clinical practice and the conduct of clinical trials; JO L 121 du 1.5.2001, p. 34.
[55] Opinion 4/2007 on the concept of personal data issued on 20 June 2007, WP 136; available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

investigator needs to know who are the patients in order to take appropriate and necessary actions for protecting their health.

Art. 29 WP, starting from the above outlined principle that "*account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify*" the data subject, reaches the conclusion that key-coded data used for clinical trials should be considered as data relating to *identifiable* data subject (and thus they are subject to the GDPR) since the identification of the patients to apply appropriate measures and health treatment in case of need is one of the purposes for which the key-coded data are processed.

In brief, it might be held that the whole processing, including the security and organizational measures adopted, is designed so that the ultimate identification of patients is something that is envisaged from the very beginning of the data processing, and is something that is planned to happen when certain circumstances occur, such as adverse effects of the medicines under trial or danger to the patients' health.

However, Art. 29 WP admits that the key-coded data are to be considered personal data for any data Controller involved in the reidentification process; however, the same conclusion may not be applicable to any other data Controller that may have access to the key-coded data.

Attention should be paid to the circumstance whether the other data controllers operate under a designed data processing that expressly excludes any reidentification of the patients, and to this purpose appropriate technical and organizational measures are implemented (such as for example cryptographic solutions, irreversible hashing measures).

In said circumstances, it is possible that reidentification of patients may be performed, for some technical or other reasons. In said case, it should be noted that reidentification is in principle excluded under any circumstance from the designing of the whole data processing, and appropriate steps have been taken to impede reidentification to take place, so if reidentification of some patients would occur, it would do so as something not supposed or unexpected to take place, as a result of unforeseeable circumstances.

In the above depicted scenario, the key-coded data processed by the original data controller should not be regarded as personal data relating to identified or identifiable data subjects, in consideration of *all the means likely reasonably to be used by the controller or by any other person*, and the data processing of said original data controller should therefore not be subject to application of the GDPR. In contrast, the data processing performed by the new data controller that performed reidentification of the patients is indeed subject to the rules of the GDPR, since this new data controller has identified the data patients and thus it has processed personal information.

In general terms, this is a matter to be considered carefully, having regard to all the specific circumstances of a certain situation, and definitively on a case-by-case basis, since general rules cannot be set forth and applied.

In case the GDPR does apply, another issue to be taken into account is that of considering that deployment of pseudonyms and key-coded data reduces the risks of breach of the data protection rights of the data subjects, thus the whole data processing, even though subject to the GDPR, might be subject to less strict conditions, due to the flexibility provided by the GDP.

3.4 Accountability: Privacy-by-design and privacy-by default

The notion of accountability is not new to privacy law and policy. It was formally introduced into data protection regulation in 1980 when it was explicitly included as a basic data protection principle in the OECD Guidelines. Since then, the accountability principle has been included in a variety of international data protection instruments as one of several core principles and is slowly (but surely) finding its way into national data protection laws.

While accountability used to be all about allocating responsibility for privacy compliance, it is now about requiring a proactive, systematic and ongoing approach to data protection and privacy compliance through the implementation of appropriate data protection measures —increasingly referred to as "privacy management programs".

Art. 24 GDPR codifies the accountability principle. In essence, it is both the respect of data processing principles and being able to demonstrate that. Indeed, the Regulation requires the controller to:

- implement appropriate technical and organisational measures (including introducing data protection by design and by default principles where relevant) to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; and
- review and update those measures where necessary through notably internal and external assessment such as privacy seals.

However, many controllers would wonder what measures they would be expected to implement. The GDPR itself provides short guidance in this regard.

Art. 24(2) provides that controllers should implement appropriate data protection policies where proportionate in relation to processing activities. Implementing those policies alone will certainly not achieve compliance with the accountability obligation. Rather, controllers will be required to implement a range of measures as needed to ensure compliance with all of their obligations under the GDPR. In addition, they must implement measures enabling them to objectively demonstrate such compliance. This requirement will need close consideration in practice. Controllers will need to thoroughly document their data protection efforts and, if requested, make such documentation available to authorities. Any data protection measures implemented will also need to be periodically reviewed and updated as appropriate.

Art. 24(3), supplemented by recital 77, provides that adherence to approved codes of conduct and certification mechanisms may help demonstrate compliance with the accountability obligation. Hence, controllers can expect codes of conducts and certification mechanisms to specify the measures required in order to comply with their accountability obligations.

The accountability provision is qualified by the so-called risk-based approach: what measures will be appropriate in each case, will depend on the nature, scope, context and purposes of the relevant processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals.

The more likely and severe the risks from the proposed processing, the more measures will be required to counteract those risks. According to recital 75, processing which could lead to physical, material, or non-

material damage would be particularly likely to constitute 'risky' processing requiring particular attention. recital 75 further provides the following examples as potentially risky processing[56]:

- processing that may give rise to discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
- processing that might deprive data subjects of their rights and freedoms or prevent them from exercising control over their personal data;
- processing of sensitive personal data or data relating to criminal convictions or offences;
- processing for purposes of profiling;
- processing of personal data of vulnerable natural persons, in particular of children; and
- processing involving a large amount of personal data and affecting a large number of data subjects.

According to recital 76, the risk must be assessed in an objective manner to determine whether there is a "risk" or a "high risk"[57]. Controllers undertaking the types of processing activities listed above or otherwise identified as 'risk' or 'high risk' would be prudent to carefully consider their obligations under the accountability provision.

The accountability principle described under art. 24 GDPR consists of two main approaches: (i) *data protection-by-design* and (ii) *data protection-by-default*.

Under the *data protection-by-design* definition, data controllers, both at the time of the determination of the means for processing and at the time of the processing itself, are required to implement appropriate technical and organisational measures —which are designed to implement data protection principles— in an effective way in order to meet the requirements of the GDPR. Doing so, controllers should adopt a risk-based approach, taking account of the risk for the rights and freedoms of natural persons resulting from a processing activity. These measures should be taken from the outset of each new processing, product, service or application. However, if a processing is actually performed, such measures should be integrated into the processing.

Data protection-by-default means, instead, that "*the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*[58]".

These definitions lead to some considerations. Firstly, the analysis of the term "appropriate measures". Pursuant to recital 74 and art. 24(1) GDPR, the controller is required to make this analysis before carrying out the processing operations, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons.

[56] See recital 75 GDPR.
[57] "*The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk*".
[58] Art. 25 GDPR.

It follows that the GDPR rather leave to the controller the chance to decide the most adequate measures according to the context of operations, and that its responsibility shall depends on all the factors mentioned above. Notwithstanding the fact that some of the measures regulated by the GDPR must be considered as compulsory, such as keeping record of the processing, appointing a Data Protection Officer, carrying out a Data Protection Impact Assessment, providing data subjects with clear and understandable information about how their data are processed.

It is also said that these measures should be effective. This implies another evaluation after the processing operations, in order to understand how much effective the measures adopted have been. Of course, the effectiveness of measures depends on the characteristics of the processing and it may be checked through different modalities, according to the level of risk involved. That is why art. 24(1) requires to review and update any measures on a regular basis.

The accountability concept does also require the controller to make sure he is able to prove the compliance of the actions adopted before the Data Protection Authority[59]. This means that accountability does not reduce the auditing powers of the Authority, but having put in place all the measures under the accountability principle underlines the proactive work of the controller and makes easier any possible investigation of the Authority. Consequently, this is an approach bringing advantages to both controllers and authorities, putting them in a reciprocal and collaborative relationship.

3.5 General principles of data processing

To have a lawful processing of personal data, they should be processed in compliance with the all principle set forth in art. 5 GDPR. These are the following:

1. Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with art. 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

[59] See also art. 5(2) GDPR.

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

Whether fairness was already explained within the Directive 95/46/EC through the concepts of loyalty and good faith that the controller is required to respect in all the steps of any personal data processing, the lawfulness has been better specified, despite being already contained in the European and national legal frameworks.

Saying that the data processing must be *lawful* implies that it should be performed according not only to applicable data protection legislation, but also to any other applicable law, regulation, and provision that may also be not a legislative act from a strict legal interpretation[60]. Lawfulness of processing relies on certain legal bases being laid down by the GDPR itself (art. 6).

The most important legal basis is the consent of data subject. Although this issue shall be analysed properly later, it is necessary underlining that consent should be freely given and the controller should be able to demonstrate that the data subject has given consent to the processing operation[61]. When consent is not applicable or it may be disproportionate for the individuals, the processing should rely on further bases, such as the compliance with legal or contractual obligation, but also the legitimate interest of the controller.

The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

The purpose principle (2), instead, states that personal data can be collected only for specified, explicit and legitimate purposes, and they cannot be processed for other purposes that are incompatible with these for which the personal data have been originally collected. The purpose principle is very important in order to determine the different data processing activities that are performed by a controller.

Basically the processing purpose defines the data processing, in the sense that in order to determine the number and kind of processing activities that are in fact carried out, it is necessary first of all to look at the reasons for which personal data are processed. The databank containing the data and the subjects processing the data are not elements of relevance, since the same subjects may be processing the same personal data that are moreover kept in the same databanks, but the processing may take place for different purposes. The fact that the purposes are different leads to the consequence that we have different data processing activities.

Moreover, the purposes for which data are processed in same cases also impact on the specific law provisions to be complied with. A simple example is if we consider the customers of a given company as data subjects.

[60] The reason of extending the legislative scenario also to laws and provisions other than applicable data protection laws should be found in the circumstance that the data protection legislation is not meant to contradict to or contrast with other applicable laws and regulations.
[61] See recital 42 GDPR.

The company may process the customers' data for purposes of performance of the contract relationship, and also for marketing activities. In said example we have two different purposes: performance of contractual obligations and marketing activities.

For the first purpose the customers' consent to the data processing is not required under the GDPR, while the consent is usually required for the other processing purpose (notably marketing activities).

The purpose principle is fundamental since it also bounds the data controller to the obligation of acting in a transparent way, in the sense that the processing purposes should always comply with what specified and made explicit by the controller in the privacy notice. Therefore, the controller cannot use the data for purposes that it has not clearly stated[62].

This rule is aimed at guaranteeing to the data subject an effective control on the processing of his data, considered under the points of view of information to be received by the data subject, of possibility for the data subject to enforce his privacy rights (for example right to access his data, to ask for deletion, updating of his data, etc.), and consciousness of the data subject when he gives his consent to the data processing.

Personal data should not only be collected and processed for specified, explicit and legitimate purposes, but should also be not further processed for purposes that are incompatible with these for which data have been originally collected and/or processed in order to guarantee consistency and lawfulness of the whole personal data processing.

The change of the data processing purposes is allowed only in accordance with the principle of compatibility that has to be assessed on a case-by-case basis.

The GDPR has made *a priori* an assessment of compatibility saying that the further processing of data for historical, statistical or scientific purposes is not incompatible with other data processing purposes, provided that the national applicable privacy laws of the relevant EU member state set forth appropriate safeguards.

Personal data must be processed to the extent strictly necessary and proportionate for the purposes established. In this sense, it should be created a kind of correlation between the personal data and the activity of processing, and they should be processed only the personal data that are strictly necessary to achieve a specific processing purpose. Accordingly, the personal data which, when assessed towards the purpose of their processing, result to be redundant or not necessary, cannot be collected or used.

In case of data that were necessary to achieve a specific processing purpose and that further begin no longer necessary since said purpose has been achieved or the way to achieve it is for any reason changed, then these data when they become unnecessary should be promptly either deleted or made anonymous.

This aspect of data processing is usually called as "data quality principle" and it also provides that personal data must be accurate and, where necessary, kept up to date.

Moreover, the controller should take every reasonable step in order to ensure that personal data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are

[62] This applies especially towards the data subject, with regard to the reasons why the data Controller wishes to process the data subject's personal data, and which is deeply linked with the right of information acknowledged to the data subject, who should always be made aware of the processing carried out on his data.

further processed, are erased or rectified. This obligation exists independently of specific orders issued by local data protection authorities or of requests of the data subject.

The rationale of the obligations relating to the rules on quality of personal data as above outlined resides in the fact that it is very important to ensure protection of the quality of personal data as information relating to the data subject, also in light of the possible damages and contrivances that may occur as a consequence of the processing, communication or spreading of incomplete or inaccurate information.

In order to comply with the data quality principle, the controller should perform periodic audits on each data processing activity that it carries out to verify that the personal data that the personal data that it process, assessed against the purposes for which said data are processed, result to be adequate, relevant and not excessive.

The principle of data quality intended as adequacy, relevance and not excess of the personal data processed should be considered in tight interaction with the data minimization and the data retention principles below considered.

As per point 5 above, the data storage principle provides that personal data must 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 were collected or for which they are further processed.

We have stated that the data quality principle provides, inter alia, that the controller may process only the personal data that result to be adequate, proportionate and not excessive if compared against the purposes for which they are processed.

Since the activity of storing personal data falls within the definition of processing of personal data under the GDPR, it follows that personal data cannot be kept forever, for an undefined period of time, since in contrast personal data may be kept (thus processed) only until the purposes for which they have been collected are achieved. After that, personal data should be immediately either deleted or made anonymous.

The GDPR could not list the specific data retention periods allowed for a lawful processing of personal data, since it would have been impossible to specify the time for which data could have been retained in relation to all the possible purposes of personal data processing.

The Regulation therefore provides a general principle (the data storage principle) that identifies the criterion to be used for a lawful storage of data, and to assess the specific period of time for which the Controller may keep the personal data that it processes.

The controller is thus charged with the burden to verify the time for which it can keep the personal data, and also to provide for solutions that allow either deletion or anonymisation of data when these are no longer necessary to the pursued purpose.

The rules above outlined that derive from the data quality principle and the data storage principle are connected one with the others, and should be considered as a whole, since each of them is prerequisite for compliance with the others, and all together they form the fundamentals on which a lawful data processing is based upon. For example, the principle of transparency allows assessing consistency of the data with the

purposes for which they are processed and also serves the purpose of determining the period of time for which data may be retained[63].

The problems related to the retention of personal data was tackled also by Art. 29 WP in the aforementioned opinion relating to search engines[64], in which it states as follows: "*If personal data are stored, the retention period should be no longer than necessary for the specific purposes of the processing. Therefore, after the end of a search session, personal data could be deleted, and continued storage therefore needs an adequate justification. However, some search engine companies seem to retain data indefinitely, which is prohibited. For each purpose, a limited retention time should be defined. Moreover, the set of personal data to be retained should not be excessive in relation to each purpose.*".

The issue of data retention period for search engines had been previously tackled with specific regard to Google that has therefore decided to limit the initial time of storage of the data on users' search activities[65]. It comes clear from the foregoing that whatever is the purpose for which data are processed, there must be an end to the retention of data, since retention of data indefinitely is against the data protection legislation.

The last principle of data processing affects the security profiles which are either technical and organizational. It consists of managing personal data while preventing them from being subject to any breach or other violations, such unauthorized accesses.

Taking into account the security and integrity of data means making adequate evaluations of any risks and the relevant security level before putting in place any processing operations, but also during the processing itself, as the protection must last for all the course of the processing. To be more accurate, the assessment of risks and security may occur after an effective violation, in order to understand if a notification to the Data Protection Authority and/or to the public should be necessary, on the basis of the risk for the rights and freedoms of individuals whose data has been involved in the breach[66].

[63] G. Buttarelli, "*Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*"; *Giuffrè; Milano;* 1997.
[64] Opinion 4/2007 on data protection issues related to search engines issued on 4 April 2008, WP 148; available at the following web address: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf.
[65] For more information, please refer to articles available in English at the following web addresses: http://news.zdnet.co.uk/internet/0,1000000097,39287254,00.htm, and http://news.zdnet.co.uk/security/0,1000000189,39288141,00.htm?r=10.
[66] For more information, see Section 8 of this deliverable.

4 Privacy roles

4.1 Data controller

4.1.1 Characteristics of data controller

According to art. 4(7) GDPR, the data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

As far as the nature of controller is concerned, there are many categories corresponding to the definition of data controller. They may regard both private and public nature, but also be included in the concepts of natural or legal person. It follows that the GDPR scope of application is not restricted to only specific categories, given any type of person, even natural and legal, may act as data controller.

It is important that the interpretation of this element should ensure the effective application of the Regulation by favouring as much as possible a clear and univocal identification of the controller in all circumstances, irrespective of whether a formal appointment has been made and publicised[67].

It may occur that companies and public bodies appoint a specific person responsible for the implementation of the processing operations. However, this natural person as well as any directors or legal representative will not be the controller but will act on behalf of the legal entity (company or public body), which will still be liable in case of breach of the principles in its capacity as controller.

Whether a natural person acting within a legal person uses data for his or her own purposes outside the scope and the possible control of the legal person's activities, he would be controller of the processing decided on, and would bear responsibility for this use of personal data. The original controller could nevertheless retain some responsibility in case the new processing occurred because of a lack of adequate security measures.

Anyway, the GDPR also admits the role of controller is played by specific substructures within the internal organization of a legal entity (such as a company or a public body), if it is clear that it effectively determines the means and the purposes of certain processing operations. For instance, the Italian Data Protection Authority had already cleared that single directions within companies, but also public minister or other administrative body, may be considered as data controller, as they have effective decisional powers regarding the processing of personal data[68].

The second crucial element of the definition of data controller refers to the determination of the means and purposes of the processing, that essentially means determining "how" and "why" personal data are processed. In analyzing these issues, the point is therefore to which level of details somebody should determine purposes and means in order to be considered as a controller.

[67] See WP169: "*It is important to stay as close as possible to the practice established both in the public and private sector by other areas of law, such as civil, administrative and criminal law. In most cases these provisions will indicate to which persons or bodies responsibilities should be allocated and will in principle help to identify who is the data controller*".
[68] See the Italian DPA's administrative provision n. 39785, 9th December 1999,

While determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means used. This is due to the fact that it may happen that the means of the processing are determined by the data processor; however, determination of the purposes is the key to understand who has the control of the processing and will be informed about the means by the processor, accordingly.

In conclusion, whoever decides on the purposes is the data controller. He is the subject of any legal situations connected with his decisions, that must come from an effective decision-making power. The determination of the means of processing can be delegated by the controller to data processor, as far as technical or organizational questions are concerned. Substantial questions which are essential to the core of lawfulness of processing are reserved to the controller. A person or entity who decides e.g. on how long data shall be stored or who shall have access to the data processed is acting as a 'controller' concerning this part of the use of data, and therefore has to comply with all controller's obligations[69].

The last element relates to the possible interaction of the controller with other subjects, given the growing likelihood of multiple actors involved in processing personal data. This relates to the role of joint controller, described in section 4.1.2 as follows.

4.1.2 Joint controllers

The definition of processing laid down by the GDPR does not exclude the possibility that different actors are involved in different operations or sets of operations upon personal data. These operations may take place simultaneously or in different stages. Indeed, the reality shows how different may be a "pluralistic control", where having all the controllers equally determining and being equally responsible for a single processing operation is only one of various types of this control.

Given this preliminary remarks, it is very important that roles and responsibilities may be easily allocated. This means that an accurate analysis of the relationship between the subjects involved and how much their decisions affect the processing should be made[70]. Unfortunately, due to the multiplicity of possible arrangements, it is not possible to finalize an exhaustive list or categorization of the different kinds of joint control.

Pursuant to art. 26 GDPR, "*where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers*". Joint control does not mean the organizations of each controller are going to be mixed; any joint controller will remain the subject in chief of its internal organization.

However, in the context of joint control the participation of the parties to the joint determination may take different forms and does not need to be equally shared[71]. While assessing how different forms may impact on the responsibilities of the processing, it should be noted that there are several degrees of interaction among parties.

For instance, the mere fact that different subjects cooperate in processing personal data does not entail that they are always joint controllers, since an exchange of data between two parties without sharing purposes or

[69] For further information, see WP169, Opinion 1/2010 on the concepts of "controller" and "processor", 2010, pag. 15.
[70] *Ibidem*, pag. 18.
[71] *Ibidem*, pag. 19.

means in a common set of operations should be considered only as a transfer or communication of data between autonomous controllers (i.e. the communication of data from a travel agency to the hotel).

On the other hand, whether parties decide to set up a shared structure to pursue their own purposes, a joint control may apply. Even though controllers want to process data for different purposes, the use of the same infrastructure whose means have been decided by each actor lead to a connected vision upon how data should be processed. That is why such relationship may be configured as joint control (i.e. A travel agency, an hotel chain and airline decide to set up an internet-based common platform in order to improve their cooperation with regard to travel reservation management)[72].

In some cases, various actors process the same personal data in a sequence. In these cases, it is likely that at micro-level the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at macro-level these processing operations should not be considered as a "set of operations" pursuing a joint purpose or using jointly defined means.

Another possible structure is the “origin-based approach”, which arises when each controller is responsible for the data it introduces in the system. This is the case of some EU-wide databases, where control —and thus the obligation to act on requests for access and rectification— is attributed on the basis of the national origin of personal data.

Another interesting scenario is provided by online social networks. To this purpose, the European Union Court of Justice ("CJEU") in the decision 5th June 2018 (C-210/16)[73] has underlined how the administrator of a fan page on Facebook has an influence on the processing of personal data of both users and non-users of Facebook by defining the parameters of his/her fan page. Using filters and defining criteria must be considered as a fundamental way contributing to the processing of the personal data of visitors to the page for the purpose of managing the advertising system of Facebook through profiling operations on the visitors (even though the administrator shall only receive statistics aimed to improve the promotion of his/her page).

The CJEU had another opportunity to analyse the concept of joint control in the decision 10th July 2018 (C-25/17)[74], where it has remarked the fact that the Jehovah's Witnesses Community does influence the processing of data of persons visited in the context of door-to-door preaching by organizing, coordinating (even through written guidelines or instructions) and encouraging such an activity[75]. Even though the community does not have access to personal data, it also receives a direct benefit from this processing, that is spreading its faith.

Having said that, according to the reasoning of the Court, the key element to understand whether the relationship between two subjects leads to joint control is appraising if both the subjects contribute to determine the purposes and means of data processing. The opportunity to define criteria upon how the processing of data should be carried out does imply exercising an influence on the processing itself, regardless of what stages of the processing the operators may be involved and the managing of identifiable or anonymous/statistical data.

Therefore, whether the advertisers or advertising agencies may concur to determine the purposes of data processing together with Yahoo —e.g., by defining criteria concerning how their targets should be reached

[72] Ibidem, pag. 19.
[73] Decision 5th June 2018 - C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*), par. 37 et seq.
[74] Decision 10th July 2018 - C-25/17 (*Tietosuojavaltuutettu*).
[75] *Ibidem*, par. 73.

through the browser on the base of profiling settings or by asking Yahoo for demographic data relating to their target audience (such as sex, age, occupation etc.), online purchasing habits and geographical data— they may be deemed as joint controllers.

Notwithstanding the fact that the reasoning of the Court in both decisions relies on the provisions of Directive 95/46/EC, which has been replaced by the GDPR, it is important the focus on the characteristic of the joint control, whose detectability should have been easier under the GDPR. Indeed, according to art. 26 GDPR the joint control must be regulated by a written agreement among the controllers involved, reflecting their roles and responsibilities toward the data subjects and describing how they process data and/or in which part they contribute for determining the purposes and means of the processing.

This includes but is not limited to responsibilities toward the data subjects in exercising their rights and providing them with the essence of the agreement together with the privacy notice in compliance with the transparency principle[76].

4.2 Data processor

According to art. 4(8) GDPR, data processor "[…] *is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*". This definition has the same profiles of the former Directive 95/46/EC and applies to any third-party subject appointed by the controller in order to assist him in processing personal data. The role of data processor is purely instrumental with regard to the purposes determined and pursued by the controller; it is possible that data processor may concur in determining the means of the processing, as he can provide the controller with his own equipment or any other tools which are necessary to carry out the processing operations.

Two basic conditions for qualifying as data processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf. This processing activity may be limited to a very specific task or context or may be more general and extended. As the processor acts on behalf of the controller, the lawfulness of the processor's data processing activity is determined by the mandate given by the controller. Therefore, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means.

However, delegation may still imply a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means.

The GDPR, in comparison to the Directive, is highly prescriptive when it comes to appointing a processor.

(a) Choice of processor

Controllers must only use processors which provide sufficient guarantees (in particular, in terms of expert knowledge, reliability and resources) to implement appropriate technical and organisational measures as required by Article 32. As it will be difficult in practice for the controller to demonstrate such due diligence, processors' adherence to an approved code of conduct (Article 40) or a certification (Article 42) can serve as sufficient guarantees for appropriate security measures taken by a processor. It is therefore likely that

[76] Even though nothing is said regarding changes to the agreement, we can say that controllers must inform the data subjects concerned.

processors adhering to such approved codes of conduct or certifications will have a tremendous advantage over other processors in the market.

(b) Data Processing Agreement (DPA)

The GDPR requires the controller and processor to enter into a written (including electronic) contract that contains certain prescribed stipulations. Firstly, the processor agreement must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subjects; and
- the obligations and rights of the controller.

But more importantly the processor agreement must expressly require the processor to:

- process personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;
- ensure that persons authorized to process personal data are subject to appropriate confidentiality obligations;
- take all applicable security measures;
- obtain the controller's consent prior to engaging a sub-processor and contractually pass on to the sub-processor the processor's data protection obligations from the processing agreement;
- assist the controller as far as possible in responding to requests by data subjects;
- assist the controller in complying with its obligations relating to data security, data breach notification, data protection impact assessments and related consultation procedures;
- at the choice of the controller, delete or return to the controller all personal data after the end of the provision of data processing services, and delete existing copies unless required by law to retain them; and
- make available to the controller all information necessary to demonstrate its compliance with the requirements for engaging a processor and allow for, or contribute to, audits (including inspections) conducted by or on behalf of the controller.

Importantly, if a processor acts outside the scope of its authority granted by the controller, in respect of the relevant processing it will be regarded as a controller and be subject to the same obligations as controllers.

In case the data processor would engage sub-contractors to assist him in providing the controller with the services offered as per the instructions of the latter, the GDPR imposes strict sub-contracting conditions.

Prior to engaging a sub-contractor in respect of specific processing activities, processors are required to obtain the specific or general written consent of the relevant controller. In the event that only a general consent has been obtained, each time the processor intends to add or change sub-contractors, it should inform the relevant controller and provide an opportunity to object. In any sub-processing contract, the initial processor must pass on to the sub-processor the data protection obligations imposed on the initial processor by the controller. If a sub-contractor fails to fulfil its data protection obligations, the initial processor remains fully liable to the controller for the performance of the other processor's obligations.

c) Liability

As far as the liability aspects are concerned, data controllers involved in processing are liable for any damage caused by the processing which is not compliant with the GDPR. Data processors, by way of comparison, are liable for damage caused by processing only if they (i) failed to comply with obligations under the GDPR specifically directed to processors; or (ii) acted outside or contrary to lawful instructions of the controller.

While the data processor's liability might seem rather narrow compared to the controller liability, this new liability of data processors is significant given that under the Directive processors were not liable for damage caused by processing directly vis-à-vis the data subjects. Also, both data controllers and processors are exempt from liability if they can prove that they are not in any way responsible for the event given rise to the damage.

Importantly, in an attempt to ensure effective compensation of data subjects, the GDPR stipulates that controllers and processors involved in the same processing will be jointly liable for the entire damage caused by such processing. While the controller/processor that pays full compensation under this regime is entitled to claim back part of the compensation from jointly liable controllers/processors (corresponding to their responsibility for the damage), the risk of being required to fully compensate data subjects is real, and recourse proceedings against other controllers/processors may be lengthy and difficult.

d) Obligation in charge of data processors

The key provision in the GDPR addressing data processors is Article 28 which directly imposes various obligations on data processors.

Firstly, processors will be subject to the same data security requirements as controllers. According to Article 32 of the GDPR, they will be required to implement appropriate technical and organizational measures to ensure a level of data security proportional to the risks inherent in the data processing for the rights and freedoms of individuals. Complying with this obligation will require a detailed assessment of various factors including the purposes of data processing activities, potential risks (such as accidental and unlawful destruction or unauthorized disclosure of, or access to, data), the state of the art of security and implementation costs.

Moreover, subject to an exemption for small organizations, processors are required to maintain a record of all categories of data processing activities carried out on behalf of a controller (art. 30 GDPR). Such records must contain, amongst others:

- details of the processor and any controllers on behalf of which the processor is acting as well as their respective representatives and Data Protection Officers (if any);
- the categories of processing carried out on behalf of each controller;
- details in respect of international data transfers (if applicable); and
- where possible, a general description of the technical and security measures implemented according to art. 32 GDPR.

Upon request, processors must make these records available to Data Protection Authorities ("DPAs").

Thirdly, processors will be required to appoint a DPO in the same way as controllers will be required to do so (art. 37), namely if their core activities consist of:

- processing operations which, by virtue of their nature, scope and/or purposes require regular and systematic monitoring of data subjects on a large scale; or
- processing on a large scale of special categories of data and data relating to criminal convictions and offences.

Furthermore, processors that are located outside of the EU will in general be required to appoint a representative within the EU (art. 27), unless an exception applies.

While processors will not be required (like controllers) to notify personal data breaches to the DPAs or affected individuals, if they become aware of a data breach they must notify such breach to the controller without undue delay to enable the controller to discharge its notification obligations. Even though the term "undue delay" has not been specified by the GDPR, it is likely that a timeframe of 72 hours will be expected by the DPAs.

Processors will also be subject to a range of additional obligations, including that they will be required to:

- cooperate, on request, with DPAs in the performance of their tasks;
- assist controllers, where necessary and upon request, in relation to data protection impact assessments and related prior consultations with DPAs; and
- return to the controller or delete data once the processing is complete.

Under the GDPR DPAs will have direct enforcement powers against processors to the extent processors fail to comply with their obligations under the GDPR. DPAs may, for example, in the execution of their investigative powers, order processors to provide information or access to personal data or premises. But they may also exercise their corrective powers and issue warnings or reprimands or require processors to bring data processing obligations into compliance with the GDPR. Last but not least, DPAs may issue significant administrative fines —according to criteria set forth in art. 83— of up to EUR 20 million against processors, or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher).

4.3 Representative of data controller or data processor

This is a role that comes out whenever the structure of art. 3(2) GDPR applies. This means that whether the controller/processor is established outside the Union, but his activities are directed to individuals located within the territory of the Union, he must appoint a representative in the Union, that is "*a natural or legal person established in the Union who […] represents the controller or processor with regard to their respective obligations under this Regulation*".

Notwithstanding the nature of the representative, that may consist of a natural or legal person, the appointment of a representative is compulsory are restricted to the following cases:

- the entity who gives the mandate (the "principal") is not a public body;
- the entity is established outside the Union and his processing activities are related to (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (ii) the monitoring of their behaviour as far as their behaviour takes place within the Union (see art. 3(2) GDPR);
- the entity carries out data processing operations on a regular basis;

- the operations involve on a large scale, the processing of special categories of data or processing of personal data relating to criminal convictions and offences;
- taking into account the nature, context, scope and purposes of the processing, it is likely to result in a risk to the rights and freedoms of natural persons.

The reason behind this role is being the nearest possible to the data subjects concerned, as well as having a more direct contact point with the Data Protection Authorities (DPAs), in case of filing claims or replying to auditing activities on behalf of the controller/processor, regardless of which third country the latter is based.

As a result, the representative, for instance, should keep —where required— the record of processing and provide the DPAs with it in case of audit. Also, the representative shall act on behalf of the principal while managing all the legal obligations the latter has under data protection law, as well as he has the capacity of filing claims whether he deems that the rights of the principal has been violated.

According to the Art. 29 WP, there is nothing against the possibility that one representative could act on behalf of several controllers or to envisage other pragmatic solutions[77]. Also, it may the preferable solution for small entities based outside the Union, as they would rely on subject with a consolidated experience on the matter.

4.4 Data protection officer (DPO): principles, tasks and guidelines

Under Art. 37, the GDPR provides the introduction of a specific figure in charge of overseeing data processing operations. However, we must underline that the concept of DPO is not new. Although Directive 95/46/EC did not expressly require any organisation to appoint a DPO, the practice of appointing such figure has nevertheless developed in several Member States over the years. Examples are Germany and Croatia both of which contain a general, non-sector specific, mandatory DPO requirement which widely applies to private and public organizations in those countries (exempting only very small organizations)[78].

The GDPR requires the designation of a DPO in three specific cases. However, it is always advisable that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly[79]. That said, Member States are also free to introduce broader national DPO requirements.

First of all, if the processing is carried out by public authorities (according the notion determined by the national law), except courts acting in their judicial capacity. There is no obligation, for instance, when a public task may be carried out not only by public authorities or bodies but also by other natural or legal persons governed by public or private law. However, in those cases the WP29 recommends, as a good practice, that: (i) private organizations carrying out public tasks or exercising public authority designate a DPO and that (ii) such a DPO's activity should also cover all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database).

[77] See WP29, *Working Document 30/05/2002*, pag. 14.

[78] Further, a handful of countries contain sector-specific DPO requirements. For example, in Finland, social welfare and healthcare service operators must appoint a DPO, while in Hungary financial institutions, public utility companies and telecoms companies must do so. In addition, other EU countries, including the Netherlands, Luxembourg, Poland and Sweden, provide for voluntary DPO appointments. These appointments (e.g., the Netherlands and Sweden) can exempt the relevant organization from certain compliance obligations such as prior notification of new processing operations to supervisory authorities (as stipulated in the Directive).

[79] When an organization designates a DPO on a voluntary basis, the same requirements under art. 37 to 39 GDPR will apply to his or her designation, position and tasks as if the designation had been mandatory.

Regarding to the private sector, data controllers and processors must designate a DPO if their core activities consist of processing operations which imply:

- regular and systematic monitoring of data subjects on a large scale, or
- processing on a large scale of special categories of data (art. 9) and data relating to criminal convictions and offences (art. 10);
- if such appointment is otherwise required by the national law.

Although the regulation does not clarify what "large scale" stands for, the Article 29 WP Guidelines on DPO[80] recommends to take account of some factors (such as the number of data subjects concerned, amount of data collected, the geographical extent of the processing and the data retention period). Some examples can be the processing of personal data for behavioural advertising by a search engine or the processing of customer data in the regular course of business by an insurance company or a bank.

As far as the regular monitoring is concerned, WP29 interprets "regular" as meaning one or more of the following:

- Ongoing or occurring at particular intervals for a particular period
- Recurring or repeated at fixed times
- Constantly or periodically taking place

WP29 interprets "systematic" as meaning one or more of the following81:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

We also as to underline that a group of undertakings may appoint a single data protection officer provided that the DPO is easily accessible from each establishment. Any other establishment can appoint a representative in order to create a stronger network on data protection issues, where the DPO would be the reference figure.

Organisations are free to choose whether to appoint an internal or external DPO. Further, DPOs do not have to exclusively work in their DPO capacity. Rather, they may also perform other tasks as long as that does not result in a conflict of interest and provided that the other tasks (even if not conflicting) leave the DPO enough time to perform the obligations as DPO (i.e., a "pro forma" appointment would not be sufficient in cases where the GDPR provides for a mandatory DPO).

As regards the qualifications of a DPO, the GDPR is not very prescriptive. It only broadly requires DPOs to possess the professional qualities and expert knowledge of data protection law and practice enabling them to fulfil their role[82]. Currently, there are not specific and recognized certification the DPO is required to accomplish. It should be also noted that the GDPR is silent on the DPO's required language skills. However, the

[80] See WP243, Guidelines on DPOs, 2016.
[81] *Ibidem.*
[82] To this purpose it is interesting the recent decision of Italian Regional Administrative Court (T.A.R.) in Friuli Venezia-Giulia, where it has been stated that having a ISO:270001 certification must not be considered as a mandatory requirement to select a DPO for a public body (T.A.R. decision n. 287/2018).

WP29 underlines that the DPO should be in a position to efficiently communicate with data subjects and cooperate with the supervisory authorities concerned. This also means that this communication should take place in the language or languages used by the supervisory authorities and the data subjects concerned.

At a minimum, and having regard to the risks associated with the processing operations, the DPO would have the following tasks:

- inform and advise the controller/processor and their employees involved in data processing of their obligations under the GDPR and other data protection laws;
- monitor compliance with the GDPR and other applicable data protection laws as well as with internal data protection policies (including assigning internal data protection responsibilities, training staff and conducting compliance audits). For instance, DPOs help controllers/processors in maintaining a record of all categories of processing activities carried out on behalf of a controller/processor, even though the liability remains in charge of the latter;
- provide advice in relation to Data Protection Impact Assessments; and
- cooperate with, act as point of contact for, and as appropriate, consult with, supervisory authorities.

The controller/processor must:

- ensure that the DPO is involved in all data protection issues properly and in a timely manner;
- provide the resources necessary for the DPO to perform his/her tasks and maintain his/her expert knowledge;
- ensure that the DPO exercises his/her functions independently and reports to the highest level of management; and
- not dismiss or penalise the DPO for performing his/her tasks.

Although Article 37(5) does not specify the professional qualities that should be considered when designating the DPO, it is a relevant element that DPOs should have expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR[83]. The DPO must have a wide knowledge of privacy issues and GDPR requirements. His knowledge should be commensurate with the complexity of the processing at stake. For example, where a data processing activity is particularly complex or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise.

Under Art. 38 the DPO should be able to perform his tasks with a sufficient degree of autonomy, that is why the GDPR establishes a minimum set of warranties to help ensure that. The controller or the processor must guarantee that the DPO is involved in all data protection issues properly and in a timely manner (such as the draft of a Data Protection Impact Assessment) as it ensures a privacy by design approach and should therefore be standard procedure within the organisation's governance.

Moreover, the controller/processor must provide the resources necessary for the DPO to perform his tasks and maintain his expert knowledge, such as giving sufficient time to fulfil his duties. This is particularly important where the DPO is appointed on a part-time basis or where the employee carries out data protection in addition to other duties[84].

[83] The WP29 deems that it would be helpful if the supervisory authorities promote adequate and regular training for DPOs.
[84] See WP243, Guidelines on DPOs, 2016.

Also, the DPO should exercises his functions independently and he cannot be dismissed or penalised for performing his tasks. Recital 97 adds that DPOs, "*whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner*". This does not exclude that the decision-making power is held by the controller, but where the controller or processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear to those making the decisions. Given that penalties are prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO, it is not admittable that a DPO cannot be dismissed for considering that a particular processing is likely to result in a high risk and advising the controller or the processor to carry out a data protection impact assessment, regardless the controller or the processor does not agree with the DPO's assessment.

The controller shall be liable for any conflict of interest arising from the assignment of tasks and powers of the DPO to any person within the internal organization. To this purpose, the Italian Data Protection Authority has said that it is preferable to avoid assigning the role of personal data protection officer to senior management (managing director; member of the board of directors; general manager, etc.), or within structures with decision-making powers regarding the purposes and methods of processing (human resources department, marketing department, financial department, IT department, etc.)[85].

DPOs are not personally responsible for non-compliance with data protection requirements. So, it is the controller or the processor who is required to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

Failure to comply with the DPO requirements set out in the GDPR may result in administrative fines of up to EUR 10,000,000, or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

[85] See https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793#7, n. 7).

5 Privacy notice

5.1 Purposes and consequences of the processing

As we have above highlighted, the data processing in general must be inspired to full transparency, especially with regard to the data subject, in order to make the data subject first of all aware that his data are being processed, and also to inform the data subject on the main features and conditions of the processing of his data. This information is important also because it enables the data subject to correctly enforce his rights under the GDPR.

It is worth it recalling that the information to the data subject is fairly considered as one of the fundamental rules of a lawful personal data processing. As pointed out in this section, whether there are several exemptions to some requirements, such as obtaining consent as legal basis to process personal data, with regard to the information requirement, instead, exemptions and limitations are very circumscribed, both at a European and also member state national level.

Article 13 of the GDPR provides a list of the mandatory information that the data subject should receive prior that the controller begins to process his personal data. The minimum list of mandatory information that the controller should provide the data subject with is as follows:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the processing is based on point (f) of art. 6(1) GDPR, the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in art. 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the list of rights the data subject may exercise to protect his personal data.

Art. 14 of the GDPR takes care of the issue of personal data that are not gathered directly from the data subject, yet form third parties, and specifies the time when the controller has to inform the data subject that it has collected personal data relating to him from other third parties. In said case the mandatory information should be given to the data subject within a reasonable period after obtaining the personal data, but at the latest within one month or, if the controller is to communicate the data to other third parties, the information to the data subject should be provided no later than the time when said disclosure of personal data takes place.

The foregoing does not apply in case the fact of providing the data subject with the mandatory information proves to be impossible or it would require a disproportionate effort or if the applicable law expressly requires the recording or disclosure of the relevant personal data. These exemptions may be set forth by member states, which must as a counterbalance provide also for appropriate safeguards. As an example of exemption under the GDPR we may recall the processing for statistical purposes or for the purposes of historical or scientific research (see art. 14(2)).

5.2 Legal bases of the processing

Art. 6 GDPR lists the six grounds for a legitimate processing that any personal data processing has to meet in order to be lawful, and it reads as follows:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 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;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;
- processing is necessary for the establishment, exercise or defence of legal claims.

From the foregoing it may be derived that the consent is one of the mandatory ground for a lawful processing of personal data, and that only when specific circumstances occur, the consent of the data subject may not be obtained.

Looking at the cases when the consent of the data subject is not required, it may be reckoned that the GDPR has strived to find a fair counterbalance between the consent requirement and the burden to obtain it that is posed on the controller. The output of the counterbalancing assessment is not asking for the data subject's consent when the above specified cases or circumstances occur since in said cases the burden on the controller would have appeared not to be justified in light of the specific personal data processing purposes pursued by the controller.

If the purposes change over time or the controller has a new purpose which he did not originally anticipate, he may not need a new lawful basis as long as his new purpose is compatible with the original purpose.

However, the GDPR specifically says this does not apply to processing based on consent. Consent must always be specific and informed. The controller need to either get fresh consent which specifically covers the new purpose, or find a different basis for the new purpose. If he does get specific consent for the new purpose, he does not need to show it is compatible.

In other cases, in order to assess whether the new purpose is compatible with the original purpose the controller should take into account at least[86]:

- any link between the initial purpose and the new purpose;
- the context in which data have been collected – in particular, relationship with the individual and what they would reasonably expect;
- the nature of the personal data —e.g., is it special category data or criminal offence data;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards —e.g., encryption or pseudonymisation.

With specific regard to special categories of data and judicial data, the extent of the lawfulness of the processing is limited to the following conditions: (i) if the data subject has given his explicit consent; (ii) when the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving the consent; (iii) when the controller processes said data to comply with obligations and specific rights in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (iv) when the processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; (v) the processing relates to data which are manifestly made public by the data subject; (vi) the processing is necessary for reasons of substantial public interest; (vii) the processing is necessary for the establishment, exercise or defence of legal claims; (viii) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services; (ix) processing is necessary for reasons of public interest in the area of public health, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Judicial data can be processed only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

5.3 Consent

Consent is subject to additional conditions under the GDPR. It should be freely given and it is clarified that consent will not be freely given if the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment and/or there is a clear imbalance between the data subject and the controller.

Consent of data subject should also be preventive and unambiguous, even when expressed through electronic means. It requires a statement or clear affirmative action of the data subject, that should include actions like ticking a box in an online context; choosing technical settings for information society services; or any other

[86] This list is not exhaustive and what the controller needs to look at depends on the particular circumstances.

statement or conduct which clearly indicates the data subject's acceptance of the proposed data processing activities. Any form of tacit consent is excluded (e.g. silence or inactivity), as well as pre-ticked boxes.

It also requires distinct ('granular') consent options for distinct processing operations. More specifically, consent must be specific, which means that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

The concept of "specific consent" is strictly connected with "informed consent". The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent.

Also, the GDPR requires an "explicit" consent from the data subject for the processing of special categories of data, profiling activities or cross-border data transfers. The term "explicit" could be interpreted according to the WP259, where it is understood as consent given in writing with a hand-written signature, as it is an easy way to make sure consent is explicit and to remove all possible doubt and potential lack of evidence in the future. Indeed, the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent (see art. 7(1)).

However, such a signed statement is not the only way to obtain explicit consent and, it cannot be said that the GDPR prescribes written and signed statements in all circumstances that require valid explicit consent. For example, in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, the use of oral statements can also be sufficiently express to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded[87].

Consent must also be specific and separable from other written agreements, clearly presented and as easily revoked as given. Data subjects must be informed of their right to withdraw consent. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels. However, each previously fulfilled processing will be considered legitimate.

Recital 43 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. It is also clear in most cases that the data subject will have no

[87] WP259, *Guidelines on Consent under Regulation 2016/679*, pag. 18-19.

realistic alternatives to accepting the processing (terms) of this controller. WP29 considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities. The same happens in the employment sector, where the dependency that results from the employer/employee relationship makes unlikely the fact that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal[88].

Specific rules will apply to children in relation to information society services. In case of age younger than 16, Internet providers and social media should ask for parental approval, unless Member State law provides for a younger age of consent (which must not be below 13). For instance, the latest Italian privacy law amending the Privacy Code (Legislative Decree n. 196/2003) has set a minimum age of 14 to give consent in relation to information society services.

While assessing the scope of this definition, WP29 also refers to case law of the CJEU. The CJEU held that *information society services* cover contracts and other services that are concluded or transmitted on-line. Where a service has two economically independent components, one being the online component, such as the offer and the acceptance of an offer in the context of the conclusion of a contract or the information relating to products or services, including marketing activities, this component is defined as an information society service, the other component being the physical delivery or distribution of goods is not covered by the notion of an information society service. The online delivery of a service would therefore fall within the scope of the term *information society service* in art. 8 GDPR.

5.4 Data retention period

According to article 5(1)(e) GDPR the data processing must have a maximum data retention period. The principle of storage limitation is codified as follows:

"*Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*".

So, even if data is collected and used fairly and lawfully, it cannot be kept for longer than the controller actually needs it.

The GDPR does not set specific time limits for different types of data. In light of the accountability approach, this is up to the controller and will depend on how long he needs the data for his specified purposes.

Ensuring that the controller erase or anonymise personal data when no longer needed will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping the controller to comply with the data minimization and accuracy principles, this also reduces the risk that he will use such data in error, to the detriment of all concerned. Indeed, personal data held for too long will, by definition, be unnecessary. It is unlikely to have a lawful basis for retention.

[88] *Ibidem*, pag. 8.

From a more practical perspective, it is inefficient to hold more personal data than the controller needed, and there may be unnecessary costs associated with storage and security. This applies, in particular, when the controller must respond to subject access requests for any personal data he holds. This may be more difficult if he is holding old data for longer than he needs.

Good practice around storage limitation —with clear policies on retention periods and erasure— is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure. Retention policies or retention schedules list the types of record or information held, what the controller uses it for, and how long he intends to keep it. They may help him establish and document standard retention periods for different categories of personal data.

6 Record of the processing operations

6.1 Goals and functioning

Under art. 30 GDPR, each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. This is one of the means required by the Regulation in order to demonstrate the controller is operating in compliance with the law. Keeping record of the processing activities, also called "data mapping", is the process of identifying, understanding and mapping out the data flows of an organization. A good data mapping (also referred to as a "Data Inventory") will provide a comprehensive overview of the data flows within, to and from an organization.

For example, a data mapping will illustrate: (i) the various categories of data held and processed by individual business units; and (2) data transfers and disclosures between different business units and to third parties, such as service providers.

In general, data mapping requires comprehensive information gathering from all business units globally, and visualization of the information gathered. The information gathering process should not be a stagnant exercise, rather it should be a dynamic consultation with the objective of gaining a comprehensive understanding of various business functions and activities in order to produce a meaningful and truthful data mapping.

Moreover, data mapping will assist controllers (and, in some instances, processors) to become compliant with various new privacy requirements as they apply to them, including:

- the requirement to maintain detailed records of an organization's data processing activities and to make these records available to supervisory authorities on request;
- the accountability requirement according to which controllers must ensure and be able to demonstrate that their processing activities are performed in compliance with the GDPR; and
- the data protection by design and by default requirements.

Data Mapping will also assist organizations assess the risks of their data processing activities for the rights and freedoms of individuals. Given the risk-based approach advocated by the GDPR, data mapping will be an important tool when assessing whether or to what extent GDPR obligations will apply will assist controllers (and, in some instances, processors) to become compliant with various new privacy requirements as they apply to them, including:

- the requirement to maintain detailed records of an organization's data processing activities and to make these records available to supervisory authorities on request;
- the accountability requirement according to which controllers must ensure and be able to demonstrate that their processing activities are performed in compliance with the GDPR; and
- the data protection by design and by default requirements.

Data mapping would also assist organizations assess the risks of their data processing activities for the rights and freedoms of individuals. Given the risk-based approach advocated by the GDPR, data mapping will be an important tool when assessing whether or to what extent GDPR obligations will apply.

However, given the vast amounts of data being collected and processed by entities these days, it would be helpful having a structured approach that considers the appointment of one person or a team committed to manage and maintain the data mapping updated; gathering relevant information, preparing the data mapping based on the gathered information. In this way, it would be useful in order to have the time to address any inefficiencies and gaps in data flows that the data mapping might reveal.

6.2 Derogations

Art. 30(5) GDPR contains a derogation to maintain a record of the processing activities. More specifically, it says that the obligation to keep a record of processing activities does not apply "*to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10*".

However, WP29 has provided some clarifications on this matter[89]. The derogation provided by Article 30(5) is not absolute. There are three alternative types of processing to which it does not apply. These are:

- Processing that is likely to result in a risk to the rights and freedoms of data subjects;
- Processing that is not occasional;
- Processing that includes special categories of data or personal data relating to criminal convictions and offences.

Therefore, although endowed with less than 250 employees, data controllers or processors who find themselves in the position of either carrying out processing likely to result in a risk (not just a high risk) to the rights of the data subjects, or processing personal data on a non-occasional basis, or processing special categories of data under art. 9(1) or data relating to criminal convictions under art. 10 are obliged to maintain the record of processing activities. However, such organizations need only maintain records of processing activities for the types of processing mentioned by art. 30(5).

For example, a small organization is likely to regularly process data regarding its employees. As a result, such processing cannot be considered "occasional" and must therefore be included in the record of processing activities. Other processing activities which are in fact "occasional", however, do not need to be included in the record of processing activities, provided they are unlikely to result in a risk to the right and freedoms of data subjects and do not involve special categories of data or personal data relating to criminal convictions and offences.

[89] WORKING PARTY 29 POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR.

7 Data Protection Impact Assessment (DPIA)

7.1 Definition and scope

Pursuant to art. 35(1) "*where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*".

When processing operations can lead to a high risk to the rights and freedoms of data subjects (because of the systematic monitoring of their conduct, or because of the large number of data subjects whose sensitive data may be processed, or even because of a combination of these and other factors), the Regulation obliges data controllers to carry out an impact assessment before initiating such a processing, with the prior consultation of the supervisory authority whether he deems that the technical and organizational measures identified to mitigate the impact of processing are not sufficient, that is, when the residual risk to the rights and freedoms of data subjects remains high.

This is one of the most important elements in the new regulatory framework, because it clearly expresses the accountability of data controllers for the processing they perform. Indeed, data controllers are required not only to ensure compliance with the provisions of the regulation, but also to adequately demonstrate how they ensure such compliance; the DPIA is a clear example of this. In this sense, it is a *data protection-by-design* measure, as it implies a prior assessment of any possible privacy-related profiles of any new project or activity.

This provision has eliminated the obligation to notify a data processing operations to DPA, given that the controller will be in charge of verifying their impact on the protection of personal data.

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. Instead, a DPIA is only required where a type of processing is "*likely to result in a high risk to the rights and freedoms of natural persons*". However, the GDPR itself does not provide many details about what would be considered a "high risk" for the rights and freedoms of individuals.

However, at the same time, the GDPR provides a non-exhaustive list of examples as to when such assessment will be required. This list, contained in the slide, regards to[90]:

- automated processing for purposes of profiling and similar activities intended to evaluate personal aspects of data subjects;
- processing on a large scale of sensitive and judicial data;
- systematic monitoring of a publicly accessible area on a large scale, such as a CCTV system in a public area.

Other cases will be indicated by supervisory authorities. Furthermore, the DPAs may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.

[90] See Art. 29 WP, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248 rev.01.

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the Art. 29 WP ha set forth the following nine criteria[91]:

1. *Evaluation or scoring*, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" (recitals 71 and 91). Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.

2. *Automated-decision making with legal or similar significant effect*: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions will be provided in the upcoming WP29 Guidelines on Profiling.

3. *Systematic monitoring*: processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area" (Article 35(3)(c))15. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

4. *Sensitive data or data of a highly personal nature*: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details.

5. *Data processed on a large scale*: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

    - the number of data subjects concerned, either as a specific number or as a proportion
    - of the relevant population;
    - the volume of data and/or the range of different data items being processed;
    - the duration, or permanence, of the data processing activity;
    - the geographical extent of the processing activity

6. *Matching or combining datasets*, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

7. *Data concerning vulnerable data subjects* (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller,

[91] *Ibidem*, pag. 8.

meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

8. *Innovative use or applying new technological or organizational solutions*, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in "accordance with the achieved state of technological knowledge" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms.

9. When the processing in itself "*prevents data subjects from exercising a right or using a service or a contract*" (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

As a general rule, the more criteria are met the more a DPIA would be necessary. However, this does not exclude the fact that a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

It is important to underline that DPIAs must be undertaken before processing operations start. However, the GDPR is silent on whether the DPIA requirement will apply in relation to processing operations already underway. So, in the absence of further guidance on this point, it is advisable that organizations identify all of their key, long-term risky processing operations (including ongoing ones) and undertake DPIAs in relation to them.

7.2 Principles and procedure

The contents of a DPIA are described in art. 35 of the GDPR as follows:

- Firstly, a systematic description of the processing operations at stake and the purposes of the processing,
- Secondly, the assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- Then, an assessment of the risks to the rights and freedoms of data subjects;
- Lastly, the measures adopted to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

The controller is responsible for ensuring that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task. The controller must also seek the advice of the DPO, where designated, while making such assessment; this advice, and the decisions taken by the controller, should be documented within

the DPIA. If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information[92].

If a DPIA carried out by a controller indicates that an envisaged processing would result in a high risk in the absence of risk-mitigating measures taken by the controller, the controller shall consult the DPA[93] prior to the processing (art. 36). Recital 94 seems to slightly soften this requirement by providing that a consultation might not be required if the controller is of the opinion that the identified risk can be mitigated by reasonable means in terms of available technologies and costs of implementation.

If the DPA considers that the processing in question would infringe the GDPR, the DPA should respond to such requests within eight weeks. However, the eight week period may be extended by six weeks in complex matters and may also be indefinitely suspended until the DPA has obtained all information requested for the purposes of a consultation. Consequently, the consultation process may take considerably longer than the projected eight week period. Further, Recital 94 clarifies that a lack of response from an DPA within the defined period will not preclude an DPA from exercising its powers, such as the power to prohibit processing operations. Hence, a lack of response to a consultation request does not confirm that an envisaged processing is GDPR-compliant nor does it mean that DPAs will not take action against such processing. This might lead to considerable uncertainties in practice.

If there are different processing with similar high risks, they can be combined.

This assessment should be reviewed and updated, if necessary. Controllers shall assess whether their data processing activities are performed in compliance with any applicable DPIA, at least when there is a change of risk represented by the processing operations.

DPIAs are a useful way for data controllers to implement data processing systems that comply with the GDPR and can be mandatory for some types of processing operations. They are scalable and can take different forms, but the GDPR sets out the basic requirements of an effective DPIA. Data controllers should see the carrying out of a DPIA as a useful and positive activity that aids legal compliance.

[92] See art. 28(3), let. f) GDPR.

[93] Some DPAs have provided a template to carry out a DPIA. For instance, the ICO provides its template at https://ico.org.uk/media/2258857/dpia-template-v1.docx.

8 Data Breach

8.1 Definition

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorized according to the following three well-known information security principles:

- Confidentiality breach: where there is an unauthorized or accidental disclosure of, or access to, personal data.
- Integrity breach: where there is an unauthorized or accidental alteration of personal data.
- Availability breach: where there is an accidental or unauthorized loss of access to, or destruction of, personal data.

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible.

Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, according to the accountability principle (art. 33(5) GDPR).

Lastly, the DPO should play a key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach (i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, WP29 recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process[94].

8.2 Notification to the Data Protection Authority: criteria and procedure

As a general rule, controllers must notify a personal data breach to the competent supervisory authority unless the breach is unlikely to result in a risk for the rights and freedoms of individuals. Importantly, those breaches that are unlikely to result in a risk for the rights and freedoms of individuals are exempt from the notification obligation providing some discretion for controllers to assess whether or not a breach must be reported. However, this exemption should be interpreted narrowly and would require the controller to demonstrate —

[94] See WP250, *Guidelines on Personal data breach notification under Regulation 2016/679*, pag. 28.

in accordance with the accountability principle— that the breach is unlikely to result in a risk for the rights and freedoms of individuals.

The GDPR requires the controller to implement all appropriate technical protection and organizational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject.

The controller should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log dat. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, art. 34. Such measures and reporting mechanisms could be detailed in the controller's incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate. The controller should also have in place arrangements with any processors the controller uses, which themselves have an obligation to notify the controller in the event of a breach.

When a controller notifies a breach to the supervisory authority, Article 33(3) states that, at the minimum, it should:

1. *describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*
2. *communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*
3. *describe the likely consequences of the personal data breach;*
4. *describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects*.

As final derogation, art. 33(1) makes it clear that breaches that are "*unlikely to result in a risk to the rights and freedoms of natural persons*" do not require notification to the supervisory authority. An example might be where personal data are already publically available and a disclosure of such data does not constitute a likely risk to the individual[95].

8.3 Notification to the data subjects involved: criteria and procedure

Data breaches must also be communicated to affected data subjects if they are likely to result in a high risk for their rights and freedoms. Importantly, notification to data subjects is not required if (art. 34(3) GDPR):

[95] See WP250, *Guidelines on Personal data breach notification under Regulation 2016/679*, pag. 18.

- *the controller adequately secured the relevant data by implementing appropriate technical and organizational protection measures (such as encryption) in relation to it;*
- *following the breach, the controller has taken measures to ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialize; or*
- *the notification of individual data subjects would require disproportionate effort - in this case a public communication of the breach would be required though*.

However, if a controller decides not to communicate a breach to the individual, art. 34(4) explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in art. 34(3) have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

Again, controller will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, he will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

According to art. 34(2) GDPR, the controller should at least provide data subjects with the following information:

- *a description of the nature of the breach;*
- *the name and contact details of the data protection officer or other contact point;*
- *a description of the likely consequences of the breach; and*
- *a description of the measures taken or proposed to be taken by the controller to address the*
- *breach, including, where appropriate, measures to mitigate its possible adverse effects.*

In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (art. 34(3)c). Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media.

WP29 in its Guidelines[96] recommends the assessment of the risk to individuals as a result of a breach should take into account the following criteria:

- The type of breach that has occurred may affect the level of risk presented to individuals.
- The nature, sensitivity, and volume of personal data. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject;
- Ease of identification of individuals: how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals;

[96] See WP250, *Guidelines on Personal data breach notification under Regulation 2016/679*, pag. 24.

- Severity of consequences for individuals: depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation;
- The number of affected individuals;
- Special characteristics of the individual (e.g. children);
- Special characteristics of the controller.

Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened[97].

[97] Annex B of WP250 provides some examples to be taken into account while assessing the risk for individuals.

9 Data subjects' rights

The GDPR retains the rights granted to data subjects under the Directive. However, the GDPR partly amends and adds to them and is more prescriptive than the Directive.

First of all, under art. 13 and 14 of the GDPR, controllers will be required to provide significantly more information about their processing activities to data subjects. Complying with the new information requirements will require controllers to update their privacy policies and to translate these requirements into internal policies and procedures in order to be prepared to comply with the new obligations, also in light of the high sanctioning threshold. On the other hand, organizations will be able to have a single EU-wide privacy policy to the extent their processing operations are the same across the EU and they make the policy available in the local language. It is also important to note that none of these rights is absolute: it is always necessary to carry out a balancing test of the different interests at stake.

In the following sections the rights of individuals will be explained in their main characteristics. For the sake of completeness, it is worthwhile underlining that data subjects must be informed of their right to:

- revoke their consent at any moment, if already given;
- lodge a complaint with the competent DPA.

9.1 Right of access

Where the right to information is intended to provide general information to individuals about the data processing operations of an organization, the right of access is intended to help individuals find out what exactly an organization knows about them, that is which specific data do they have, how and why are they used and with whom have they been shared.

Under art. 15 GDPR, data subjects are allowed to request the confirmation from the organization if data is being processed about them, as well as the following detailed information: (i) Purposes of processing, (ii) Categories of personal data, (iii) Recipients of the data, (iv) Retention scheme applied to the data, (v) Existence of further data subject rights, (vi) The right to lodge a complaint with the DPA, (vii) Source of the data, (viii) Any profiling that is undertaken with the data, and (ix) Third country transfers, including safeguards.

Companies are allowed to limit their response to what was requested by the data subject. A copy of the data shall be provided at no cost, in principle in the same way the access request was filed. For an electronic request an electronic copy of the data would therefore suffice. However, for further copies beyond the first one a reasonable fee could be charged, for example the costs of the photocopies in case of a hard copy access request.

Controllers must respond to access requests without undue delay, and at the latest within one month, subject to a two-month extension for complex requests or large numbers of requests. If a delay occurs, the data subject needs to be informed about it. The extension of the deadline is possible with two times one month, and not with two months in one go[98].

[98] See Nymity DSR Handbook, *Data Subject Rights Handbook*, 2018, pag. 10.

Also, controllers should use all reasonable measures to verify the identity of data subjects requesting access before granting access, as it would put in danger the identifiability of different data subjects and their personal data.

9.2 Right to rectification

The data subjects have the right to request the data controller to update or rectify their inaccurate or incomplete personal data concerning them. This right reflects the data quality principle, according to which the controller has the duty to control the data to be accurate and up-to-date.

Art. 16 GDPR says "*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement*". What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort controller should put into checking its accuracy[99] and, if necessary, taking steps to rectify it.

Usually this right is exercised following an access request, but it is not a necessary precondition. If an individual already knows the data held by the organization is wrong (for example because mail was received at the wrong address) he can also file the correction request immediately.

Even though having accurate data is useful for the controller, he can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. In that case the controller is required to justify his decision and may request a "reasonable fee" to deal with the request.

9.3 Right to erasure

The GDPR also contains a right to erasure (also referred to as a "*right to be forgotten*"), that is the right to deletion or erasure, that allows individuals to request that, in certain situations, their data are removed from the database of the organization. Therefore, data controllers will be required to erase personal data upon request and without undue delay if one of the following grounds is met:

- the data is no longer necessary for the purpose for which it was collected or otherwise processed;
- the data subject withdraws consent on which processing is being based and no other legal processing ground can be relied on;
- the data subject validly objects to the processing pursuant to art. 21;
- the data has been unlawfully processed;
- the erasure is required for compliance with a legal obligation under Union or Member State law; or
- data has been collected in relation to the offering of information society services to a child.

The circumstances in which personal data must be erased are not all new and partially exist already under national data protection legislation (such as in Germany and Italy). The above also does not codify a broad

[99] The GDPR does not provide a definition of "accuracy". However, the UK Data Protection Act 2018 (DPA 2018) states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact. See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/.

right to be forgotten as was established by the CJEU in the Google Spain v Costeja decision[100], where was configured a non-absolute right for individuals to get their information delisted from search engines, if the data could not be removed from the original source and were no longer considered to be relevant.

Importantly, where controllers have publicized personal data that they are obliged to erase, they are required to take reasonable steps (taking into account available technology and costs) to inform other controllers who are processing the data, that the data subject has requested the erasure of any links to, or copy or replication of, such data.

The right to erasure is subject to a number of exemptions, including where the data processing is necessary for exercising the right to freedom of expression and information, for compliance with a legal obligation or for the establishment, exercise or defence of legal claims.

9.4 Right to restriction of the processing

Under art. 18 GDPR data subjects also have the right to restrict the processing of personal data if the data itself or the lawfulness of the processing are contested, as follows:

- a data subject contests the accuracy of personal data and the controller is in the process of verifying the accuracy of the data;
- processing is unlawful but the data subject requests the restriction of the processing rather than an erasure of the data;
- the controller no longer needs the personal data for the purposes of processing but the data subject requires the data for the establishment, exercise or defence of legal claim; or
- the data subject has objected to the processing and a decision is pending as to whether the controller may continue to process the data on the basis of legitimate interests.

In case of such a processing restriction, controllers may store the relevant data but may no longer in any other way process it, except with the data subject's consent, for the establishment, exercise or defence of legal claims or for reasons of important public interest. Before processing restrictions are lifted, the controller must inform the data subject accordingly.

9.5 Right to data portability

The right to data portability is enshrined in art. 20 GDPR. Individuals are entitled to take their data from one organisation to the other:

- *If processing is based on consent or contract; and*
- *The data are processed by automated means*[101].

If either of these criteria is not met, the right to data portability does not apply. Of course, the individual would still be able to obtain a copy of his/her data under the right of access, but that would leave out one advantage.

[100] CJEU, Google Spain v AEPD and Mario Costeja González, C-131/12, 13 May 2014, par. 88: "*The operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful*".

[101] See Nymity DSR Handbook, *Data Subject Rights Handbook*, 2018, pag. 25.

Data portability requires the copy of the data to be provided in an electronic, machine-readable format, either to the individual, or, preferably, directly to the new service provider.

Although the right to data portability is limited (e.g., it only applies where a data subject has proactively provided personal data to a controller and the data is processed by automated means and on the basis of consent or in performance of a contract), this right requires many controllers to implement technical processes to honour this right and might well result in a requirement to hand over valuable personal data to a competitor. However, while controllers are encouraged to develop interoperable formats that enable data portability, they are not strictly required to adopt processing systems that are technically compatible.

9.6 Right to objection

Under the GDPR (art. 21), data subjects have broader rights to object to data processing activities. Specifically, they are able to object to processing of their personal data based on legitimate interests without having to demonstrate compelling legitimate grounds for such objection (as it was required under the Directive). Rather, where the controller wishes to continue to process such data despite an objection, it will be required to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or to demonstrate that the processing is necessary for the establishment, exercise or defence of a legal claim.

Data subjects retain their right to object to processing of their personal data for direct marketing purposes (including the right to object to profiling related to direct marketing)[102].

[102] See art. 21(2) GDPR.

10 International transfer of data

10.1 Legal bases

One of the greatest achievement of the GDPR is having created a consolidated area where the free movement of personal data is ensured, as a consequences of having a unique privacy legal framework within the Union and the European Economic Area ("EEA")[103]. On the other hand, for all the third countries outside the Union and the EEA, the GDPR provides different tools to frame data transfers.

Firstly, a transfer may take place where the EU Commission has decided that the third country in question ensures an adequate level of protection (art. 45 GDPR). In these cases, no specific authorisation of the transfer by supervisory authorities will be required.

Even though this mechanism was already regulated by the Directive, the rules for assessing the adequacy of the level of privacy protection in a given country, territory, sector or international organization are much more prescriptive than those under the Directive.

Importantly, in order to be given adequacy status, a third country is expected to offer guarantees that ensure a level of data protection essentially equivalent to that guaranteed within the EU. In particular, it should ensure effective independent data protection supervision and provide for cooperation mechanisms with European DPAs. Further, data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress (art. 45(2)).

Adequacy decisions will be subject to a periodic review (at least every four years) and may be repealed, amended or suspended by the Commission if the latter concludes that an adequate level of data protection is no longer ensured. Indeed, art. 45(4) says that "*the Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted*".

a) Standard Contractual Clauses

The European Commission may authorize the transfer of personal data towards third countries without an adequate data protection level upon enforcement of certain Standard Contractual Clauses (SCCs) offering sufficient safeguards.

The "Model Contract" is the set of contract provisions contained in the decision of the European Commission, and until the time of drafting of this deliverable, the European Commission has issued three sets of Model Contract: Commission Decision (2010/87/UE) of 5 February 2010 on the transfer towards data processors established in third countries and repealing the former Decision 2002/16/EC; Commission Decision 2001/497/EC of 15 June 2001 and Commission Decision C(2004)5271 of 27 December 2004 on the transfer towards Controllers established in third countries. If data controller is making a restricted transfer to another controller, you can choose which of the two set of clauses to use, depending on which best suits the business arrangements.

[103] The GDPR was among 69 EU legal acts incorporated into the EEA Agreement by the EEA Joint Committee in Brussels on 6 July 2018 http://www.efta.int/media/documents/legal-texts/eea/the-eea-agreement/Annexes%20to%20the%20Agreement/annex11.pdf.

The Commission plans to update the existing standard contractual clauses for the GDPR. Until then, controller can still enter into contracts which include the Directive-based standard contractual clauses[104].

When entering into a new contract, the controller must use the SCCs in their entirety and without amendment. He can include additional clauses on business related issues, provided that they do not contradict the what set forth in SCCs. He can also add parties (i.e. additional data importers or exporters) provided they are also bound by the standard contractual clauses.

b) Binding Corporate Rules

BCRs, also known as "Binding Corporate Rules", are meant to allow the transfer of personal data from the territory of a Member State to third countries between entities belonging to the same group of undertakings. Considering the value that today the flow of data has for international trade, it is easy to understand how the attention of large companies has been directed in the search for a mechanism that could facilitate the circulation even in countries outside the EU through specific agreements that could provide for the concrete case the appropriate guarantees that are lacking in the legislation of the country of establishment.

Whether the SCCs are standardized tools, BCRs "*needs to be tailor-made to the particular needs of a given corporation*" and are "*based on the organisation having a sufficiently satisfactory and robust data protection regime already in place within the group or introducing the necessary measures to ensure that the systems in place meet the BCR requirements*"[105].

Since 2012, there have been two different types: the BCRs for the Controller and the BCRs for the Processor (BCR-P). The first are the traditional ones, formulated to allow a group of companies to process data even in members that are part of it and operate outside Europe, while the second was created following the establishment of the SCCs controller-to-processor, and aims to allow the transfer of data to the members of a group that do not act as the controller, but as a data processor.

BCR-P have been officially recognized by Art. 29 WP in a specific document, the WP195, which identifies the relevant principles and rules, as well as the form to request approval[106] of the entities involved, from which it must emerge clearly that the participants of the group undertake to comply with the principles contained in the BCR-P and are held accountable to the owner of the treatment for violation of its instructions. This does not mean that the data controller is not obliged to check that the BCR-P contains adequate guarantees for the data transferred to and processed by the data controller.

c) Certifications and Codes of Conduct

Under art. 46(2), let. e and f, the controller can make a restricted transfer if the receiver has signed up to a code of conduct or has a certification, which has been approved by a supervisory authority. The code of conduct or the certification must include appropriate safeguards to protect the rights of individuals whose personal data transferred, and which can be directly enforced.

[104] Existing contracts incorporating standard contractual clauses can continue to be used for restricted transfers (even once the Commission has adopted GDPR standard contractual clauses).
[105] See WP204, *Explanatory document on the Processor Binding Corporate Rules*, 2013.
[106] See also WP 265, *Recommendation on the approval of the Processor Binding Corporate Rules form*, 2018.

The GDPR endorses the use of approved codes of conduct or certifications to demonstrate compliance with its requirements. However, this option is newly introduced by the GDPR and no approved codes of conduct are yet in use.

d) EU-US Privacy Shield legal framework

With specific regard to the transfer of personal data to the U.S., the former framework relied on the Decision 2000/520/EC of the EU Commission which approved the "Safe Harbour" scheme to legitimate any data flows towards U.S. However, after the CJEU decision C-362/14 6th October 2015, the so-called "Schrems v. Data Protection Commissioner", the Safe Harbour has been invalidated.

On 2nd February 2016 an agreement was reached between the European Union and the United States that leaded to a new framework, the so-called EU-US Privacy Shield, published on July 12, 2016. In a nutshell, it was the result of a rapid process of renegotiation, necessary in an increasingly vital context both for its economic aspects, and for the protection of security and privacy, which in this period of time has been the victim of a "regulatory hole" not indifferent.

The text can be divided into two parts: a list of the Privacy Principles (Annex 2) and the declarations and commitments adopted by the US Government and the US Trade and Justice Departments.

The first part shows a greater deepening of the issue of protection than the Safe Harbour. This is reflected in a more careful focus on risk, an increase in the level of responsibility of data processors, the definition of specific procedures for complaints regarding unlawful treatment, which can be submitted both by European citizens and by the authorities, and finally in the adoption of a system of active and ex officio monitoring by the U.S. authorities, in order to verify whether member companies are actually complying with the provisions of the Privacy Shield. The principles outlined are 7 (with 16 additional principles): *notice, choice, onward transfer, security, data integrity, access, enforcement*.

The second part concerns access to and use of information by US authorities, which, unlike the Safe Harbour, is subject to restrictions both when the aim is that of national security, and for the public interest and law enforcement.

Last important innovation has been the creation of an ad hoc figure, the *Privacy Shield Ombudsperson*[107], a body created within the US Department of State, representing the point of contact between European authorities and American institutions, being responsible for providing a response to complaints made by European citizens to their national authorities about possible violations committed by U.S. intelligence agencies.

10.2 Derogations pursuant to art. 49 GDPR

If the controller is making a restricted transfer that is not covered by an adequacy decision, nor an appropriate safeguard, then you can only make that transfer if it is covered by one of the 'exceptions' set out in Article 49 of the GDPR. He should only use these as true 'exceptions' from the general rule that you should not make a restricted transfer unless it is covered by an adequacy decision or there are appropriate safeguards in place.

The derogations set forth in art. 49 are the following:

[107] For further information see https://www.state.gov/e/privacyshield/ombud/.

- *The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.*
- *the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;*
- *the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;*
- *the transfer is necessary for important reasons of public interest;*
- *the transfer is necessary for the establishment, exercise or defense of legal claims;*
- *the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;*
- *the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case*.

The above derogations largely mirror those provided for in the Directive, except that consent is now required to be explicit and the data subject must be informed about the risks resulting from the transfer prior to consenting.

The GDPR also provides for one new very limited "last resort" derogation. Essentially, if a proposed transfer cannot be based on an adequacy decision, appropriate safeguards or one of the above derogations, a transfer may take place if it is not repetitive (i.e., occasional), concerns only a limited number of data subjects and is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject. But, as a further condition, the controller must adduce suitable safeguards to protect the personal data (having assessed all the circumstances surrounding the data transfer) and inform the DPA and the data subjects about the transfer.

11 Sanctions

In order to strengthen and harmonize administrative penalties for data protection infringements, the GDPR sets the upper limit and criteria for determining fines which are then finally determined by the competent DPA in each individual case.

Importantly, the GDPR expressly states that as a general rule (in order to strengthen enforcement of the GDPR rules), penalties and administrative fines should be imposed for any infringement of the GDPR in addition to, or instead of, appropriate measures imposed by the DPA. The exceptions are minor infringements and cases in which a fine would constitute a disproportionate burden to a natural person. In those cases, a reprimand may be issued instead of a fine. Therefore, the imposition of fines is likely to become the norm.

Article 83 (2) provides a list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine.

Firstly, once an infringement has been established the DPA should impose an equivalent sanction, that is consistent with the gravity of the violation. Also, such violations must be effective, proportionate and dissuasive. To assess what is effective, proportional and dissuasive in each case it will be necessary to also reflect the objective pursued by the corrective measure chosen, that is either to re-establish compliance with the rules, or to punish unlawful behaviour[108]. It is clear that any DPA will conduct an analysis based on a specific evaluation of each case, in order to better understand the proportionate content of the sanction, event through a reciprocal information exchange among DPAs.

The GDPR provides the following rules for determining the scope of administrative fines to be imposed:

- The imposition of administrative fines shall in each case be effective, proportionate and dissuasive.
- Depending on the circumstances of each individual case, administrative fines should be imposed in addition to, or instead of, other corrective measures.

Various factors need to be considered when determining whether to impose a fine and of what amount, including in particular:

- the nature, gravity and duration of the infringement;
- the intentional or negligent character of the infringement;
- actions taken to mitigate damage suffered;
- the degree of responsibility or any relevant previous infringements;
- the manner in which the infringement became known to the DPA (in particular whether the controller/ processor notified the DPA);
- the degree of cooperation with the DPA in order to remedy the infringement and mitigate the adverse effects;
- compliance with measures previously ordered against the controller/ processor;
- adherence to a code of conduct; and
- any other aggravating or mitigating factors (such as financial benefits gained).

[108] See WP253, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 2018, pag. 6

- If a controller or processor violates several provisions of the GDPR in relation to the same or linked processing operations, the total amount of the fine may not exceed the amount specified for the gravest violation.

The GDPR imposes a two-tier fine system.

1. Tier-one infringements are subject to administrative fines of up to EUR 10,000,000, or in the case of an undertaking, up to 2% of the worldwide annual turnover of the preceding financial year (whichever is higher). One example is failure to obtain parental consent where information society services are offered to children below the age of consent (Art. 8) failure to obtain parental consent where information society services are offered to children below the age of consent (Art. 8); also, failure to inform data subjects that personal information about them is de-identified (Art. 11).
2. Tier-two infringements are subject to administrative fines of up to EUR 20,000,000, or in the case of an undertaking, up to 4% of the worldwide annual turnover of the preceding financial year (whichever is higher). For instance, failure to comply with data subjects' rights or failure to comply with cross-border transfer principles (Art. 44-49).

In the context of determining fines under EU competition law, an "undertaking" refers to the entities that are held liable for the infringement. This may include multiple separate legal entities and, in particular, a parent may be held liable for the actions of a subsidiary if the parent exercised "decisive influence" over the subsidiary (even if the parent did not actively participate in the infringement). Determining whether a parent exercised decisive influence requires a fact-based analysis (although there is a presumption that a parent will be held liable in respect of its wholly-owned subsidiary). If a parent is held liable then the parent's turnover will be used to calculate the fine, i.e. the 2%/4% fine cap will apply to the parent's turnover, thereby significantly increasing the potential level of the fine.

Reflections on the questions such as those provided in the previous section will help supervisory authorities identify, from the relevant facts of the case, those criteria which are most useful in reaching a decision on whether to impose an appropriate administrative fine in addition to or instead of other measures under Article 58. Taking into account the context provided by such assessment, the supervisory authority will identify the most effective, proportionate and dissuasive corrective measure to respond to the breach.

12 Legal claims and compensation of damages

12.1 Principles

According to art. 77 GDPR, the data subject has the right to lodge a complaint with the competent DPA, as also mentioned in art. 13. The DPA is required to analyse the claim, evaluating all the alleged infringements or critical aspects, and decide if its assessment may lead to sanctions or the mere rejection of the claim.

This not excludes the possibility for anyone concerned by the DPA's decision, to request an effective judicial remedy against such a legally binding decision, without prejudice to any other administrative or non-judicial remedy (see art. 78).

Alternatively, data subjects may decide to not proceed before DPA, but a judicial court. According to art. 79, "*Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers*".

Whether it is ascertained the existence of a material or non-material damage as a result of an infringement of the GDPR, the data subject shall have the right to receive compensation from the controller or processor for the damage suffered.

As a general rule, the controller has the liability for the damage caused by processing which infringes the GDPR. However, "*a processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller*" (see art. 82(2) GDPR).

12.2 Data Protection Authority

Each Member State is required to establish one or more independent public authorities responsible for monitoring compliance with, and enforcing the provisions of, the GDPR. The GDPR goes further than that and clarifies that each such supervisory authority should be provided with the financial, human and technical resources, premises and infrastructure necessary for the effective performance of their tasks. Importantly, those supervisory authorities who previously relied on notification fees as a resource will no longer have this income stream available. It remains to be seen whether the GDPR will result in better equipped and more active regulators.

The GDPR expressly states that, in order to ensure consistent monitoring and enforcement, DPAs should have the same tasks and effective powers across Member States. From an enforcement perspective, these powers include investigative powers, corrective powers and sanctions, as well as powers to bring infringements of the GDPR to the attention of judicial authorities and/or engage in legal proceedings to enforce the provisions of the GDPR. As a general rule, enforcement measures must be appropriate, necessary and proportionate in view of each individual case. DPAs has less discretion about enforcement rules, but critically they retain discretion about application of the provisions.

The investigative powers include, amongst others, powers to[109]:

- order controllers and processors to provide information;
- carry out investigations in the form of data protection audits;
- obtain from controllers or processors access to personal data and other information; and
- obtain access to any controller/ processor premises (which power should be exercised in compliance with national procedural requirements, such as obtaining prior judicial authorisation).

The corrective powers include, amongst others, powers to:

- issue warnings to controllers/ processors that intended processing operations are likely to infringe the GDPR;
- issue reprimands to controllers/ processors where processing operations infringe the GDPR;
- order controllers/ processors to bring processing operations into compliance with the GDPR;
- order controllers to communicate personal data breaches to data subjects;
- impose a temporary or definitive limitation (including a ban) on processing;
- impose administrative fines (in addition or instead of any other corrective measures); and
- order the suspension of international data flows.

12.3 Lead Authority and One-stop-shop mechanism

Under the GDPR, each Member State will continue to be required to establish one or more independent public authorities responsible for monitoring and enforcing the application of the GDPR. Existing DPAs (data protection authorities) are likely to play that role in all Member States. However, the GDPR contains new rules regarding the competencies and cooperation between such DPAs.

As a general rule, each DPA will be competent to perform the tasks assigned to it and exercise the powers conferred on it on the territory of its Member State (art. 55). According to Recital 122, this should be particularly the case where the processing:

- is carried out in the context of the activities of an establishment of the controller/ processor on its territory;
- is carried out by public authorities of that Member State;
- affects data subjects on its territory; or
- is carried out by a controller/ processor not established in the EU when targeting data subjects on its territory.

However, in cases of cross-border processing, generally only the DPA of the main or single establishment of the controller/ processor will be competent to act as *lead authority*, subject to an obligation to cooperate with other *concerned DPAs* (Article 56(1)). This is the *One-Stop-Shop* principle, which implies that the supervisory authority in the jurisdiction of the main or single establishment of the controller or processor will be the lead authority, even though each national authorities remain competent to handle a complaint or a possible infringement related only to an establishment in its Member State or substantially affects data subjects only in its Member State.

[109] See art. 57 GDPR

The term "cross-border processing" is defined in art. 4(23) GDPR. In a nutshell, it comprises: (i) data processing by controllers/ processors established in more than one EU Member State which processing takes place in the context of the activities of establishments in more than one Member State; and (ii) data processing which takes place in the context of the activities of a single establishment of a controller/ processor in the EU but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

By way of derogation from this rule for cross-border processing, each DPA shall be competent to handle a complaint lodged with it or a possible infringement of the GDPR if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State (art. 56(2)). So, there will be room for local DPAs to argue that they will be competent in cross-border processing cases even though they would technically not qualify as "lead DPA". The final decision as to who will handle the matter in these cases rests with the lead DPA (art. 56(3)). Further, the OSS mechanism does not apply in cases of data processing by public authorities or private bodies acting in the public interest (art. 55(2), Recital 128).

The competent lead DPA will be the DPA of the main establishment or of a single establishment of the controller or processor engaging in the cross-border processing in question.

- The main establishment of a controller with establishments in more than one Member State is generally the place of its central administration within the EU. However, if the decisions on the purposes and means of processing are taken in another establishment of the controller in the EU and the latter establishment has the power to have such decisions implemented, then that other establishment is to be considered the main establishment.
- The main establishment of a processor with establishments in more than one Member State is also generally the place of its central administration in the EU. If a processor has no such central administration in the EU, its main establishment is its establishment in the EU where the main processing activities in the context of the activities of an establishment of the processor take place to the extent the processor is subject to specific obligations under the GDPR.

A DPA will be a "concerned DPA" (art. 4(22) GDPR) in the following cases:

- a relevant controller or processor has an establishment on the territory of its Member State;
- data subjects residing on the territory of its Member State are substantially affected or likely to be substantially affected by a processing in question; or
- a complaint has been lodged with it (regardless whether that complaint has been lodged by a data subject residing in that Member State or elsewhere).

In practice, the designation of lead DPAs and concerned DPAs as well as their cooperation will be challenging processes. Recognizing this, the Art. 29 Working Party has already announced that preparing the OSS and consistency mechanism and coming to precise conclusions on how these mechanisms are intended to work will be one of its key priorities during 2016.

Article 60 sets out detailed rules for lead DPAs and concerned DPAs to cooperate in cases of cross-border processing. For example, they shall exchange information, the concerned DPA shall provide assistance to the lead DPA upon request (e.g., by conducting inspections or investigations), the lead DPA shall keep concerned DPAs informed on a particular matter and seek their input on draft decisions. Overall, the lead DPA should closely involve and coordinate the concerned DPAs in the decision-making process. Decisions are to be agreed jointly between the lead DPA and concerned DPAs following a complex process for sharing draft decisions,

taking into account relevant and reasoned objections by concerned DPAs in relation to them and adopting mutually agreed decisions. Where DPAs have conflicting views as to which DPA is competent to act or cannot jointly agree a decision, the matter will be referred to the European Data Protection Board (EPDB) for resolution. This cooperation requirement is subject to an urgency exception. A concerned DPA may immediately adopt provisional measures intended to produce legal effects on its own territory and valid for no more than three months if it has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects (art. 60(11) and 66). Such urgent need to act may arise, for example, because otherwise the enforcement of a right of a data subject could be considerably impeded (Recital 137). It remains to be seen how this exception will be interpreted.

12.4 European Data Protection Board (EDPB)

The European Data Protection Board (EDPB)[110] is an independent advisory body with legal personality, replacing the Art. 29 WP, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities. It is based in Brussels and has been regulated under art. 68 et seq. GDPR.

The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS). The supervisory authorities of the EFTA EEA States are also members with regard to the GDPR related matters and without the right to vote and being elected as chair or deputy chairs. The European Commission and, with regard to the GDPR related matters, the EFTA Surveillance Authority has the right to participate in the activities and meetings of the Board without voting right.

The EDPB aims to ensure the consistent application in the European Union of the General Data Protection Regulation and of the European Law Enforcement Directive (2016/680). In doing so, the EPDB plays a key role in the "*consistency mechanism*" (art. 63 to 67 GDPR) intended to ensure a consistent application of the GDPR across the EU (one of the major downfalls of the regime under the Directive 95/46/EC).

One aspect of the consistency mechanism is the referral of disputes between DPAs on particular matters to the EDPB for resolution. Further, according to the consistency mechanism, DPAs must obtain the EDPB's opinion before they adopt any of the measures listed in art. 64(1), such as Binding Corporate Rules, standard contractual clauses or lists of processing operations that fall under the DPIA requirement. While the GDPR sets out a complex consultation process for consultation between DPAs and the EDPB, the EDPB will ultimately retain the last word and be able to issue a binding opinion in case of disagreement.

[110] For more information see https://edpb.europa.eu/edpb_en.

13 GDPR alignment laws

In the following, the current status of National alignment laws is summarised for the 28 Member States[111].

Austria

Data Protection Implementation Act 2018 (31 July 2017)

Belgium[112]

Law of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal Data (5 September 2018).

Law establishing Data Protection Authority (3 December 2017).

Bulgaria

Data Protection Act (still draft) (30 April 2018)

Croatia

The Law on Implementation of the General Data Protection Agreement (3 May 2018)

Cyprus

Law Providing protection of natural persons against the processing of personal data and the free movement of this data (21 July 2018)

Czech Republic

Draft law on the processing of personal data

Denmark

Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act) (23 May 2018)

Estonia

Personal data protection bill 616 SE (still draft)

[111] For more information see https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/.

[112] There is a legal framework essentially composed by: (i) The "Institutional Law" (Law of 3 December 2017 establishing the Data Protection Authority); (ii) The "Substantive Law" (Law of 30 July 2018 on the protection of natural persons with regard to the processing of their personal data); (iii) The "Collective Redress Law" (Law of 30 July 2018 with various provisions on economic matters, which introduces collective redress action); (iv) The "Information Security Law" (Law of 5 September 2018 the creation of an Information Security Committee); and (v) The "Camera Law" (Law of 21 March 2018 modifying the Law of 21 March 2017 on the installation and use of cameras).

Formatiert: Englisch (Großbritannien)

Finland

Government proposal to Parliament for supplementing the EU General Data Protection Regulation (1 March 2018)

France

Law concerning the protection of personal data (20 June 2018)

Germany

The German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (5 July 2017)

Greece

Draft law on the protection of data (20 February 2018), has already been subject to public consultation; its submission to the Parliament for being voted is still pending.

Hungary

Act on the right to information self-determination and freedom of information 2011 CXII. law for legal harmonization (20 June 2018).

Draft bill on the right to information self-determination and freedom of information (20 June 2018).

Ireland

Data Protection Act 2018 (24 May 2018)

Italy

Provisions for the adaptation of national legislation to the provisions of the GDPR. Legislative Decree n. 101/2018 (10 August 2018)

Latvia

Personal Data Processing Law (21 June 2018)

Lithuania

Law on the Protection of Personal Data (16 July 2018)

Luxembourg

Law of 1 August 2018 on the organization of the National Commission for Data Protection and the General Scheme on Data Protection (16 August 2018)

Malta

Data Protection Act (28 May 2018)

The Netherlands

Law Implementing the General Data Protection Regulation (16 May 2018)

Poland

Law on the protection of personal data (24 May 2018)

Portugal

Proposed Law No. 120 / Xiii (3) ensures the implementation, in the national legal order, of regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal and free data circulation of these data (26 March 2018)

Romania

Law 190/2018 on measures to implement regulations of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing the EU Directive 95/46 (31 July 2018)

Slovakia

Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll. (30 January 2018)

Slovenia

Proposal of the Law on Personal Data Protection (4 April 2018)

Spain

5/2018 on urgent measures for the adaptation of Spanish Law to European Union regulations on data protection (31 July 2018)

Sweden

Regulation (2018: 219) with additional provisions to the EU Data Protection Ordinance (19 April 2018)

UK

Data Protection Act (23 May 2018)