INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

JUST-JTRA-EJTR-AG-2016
Action grants to support European judicial training
JUSTICE PROGRAMME
GA No. 763866

INtroduction of the data protection reFORM to the judicial system
INFORM

WP2: Data Protection regulatory review & training material elaboration

D2.11 Data Protection Glossary

Lead partner: University of Cyprus

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [1]

Project co-funded by the European Commission within the JUST Programme		
Dissemination Level:		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version 1	Originated by: UCY/UNIBA	January 11th 2018
Version 1	Reviewed by: Matthias Eichfeld, University of Göttingen	January 17th 2018
Version 1	Reviewed by: George Dimitrov, Law and Internet Foundation	January 17th 2018

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Introduction

The purpose of this Glossary is to assemble and explain the principal terms concerning data protection issues relevant to the administration of justice system and more specifically as they relate to the introduction of data protection reform to the judicial systems of EU Member States, in the light of the new generation of data protection instruments, namely the General Data Protection Regulation (GDPR) and the *Directive 2016/680 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*. These instruments (referred to in the Glossary respectively as *"the Regulation"* and *"the Directive"*) have primarily replaced Directive 95/46 and Council Framework Decision 2008/977/JHA respectively. The Regulation and the Directive have on the one hand introduced new concepts into the field of European data protection law and, on the other hand, updated the meaning and systematized the employment of other concepts. They are also leading to a further homogenization of European data protection law, reducing the diversity among Member States' data protection laws and expanding the scope of data protection in important areas such as the administration of justice.

The policies underlying EU data protection reform, notably optimising harmonization of data protection regimes across the Union; allowing for the showcasing of best practices; and, especially, putting the emphasis on compliance and pre-emption of infringing behaviour, are reflected in this Glossary. The Glossary draws from the Regulation and the Directive as its primary sources, but it has also benefited significantly from the background research undertaken in the course of the INFORM project, especially within Workstream 2, as well as more broadly, European scholarship on data protection policy and practice.

The Glossary was undertaken by legal experts from the University of Cyprus (UCY) and Comenius University of Bratislava (UNIBA). The authors of the Glossary are: Elvira Pallikarou, Nikitas Hatzimihail (UCY), Dusan Soltes, Silvia Trelova, Daniela Novackova, Martina Drahoseva (UNIBA). The authors wish to thank Matthias Eichfeld from the University of Göttingen and his team for guidance and valuable feedback in various stages of the undertaking.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Table of contents

Introduction 3

Terms 6

Access (right of) 6

Accountability *(principle of)* 7

Accuracy *(principle of)* 8

Biometric data 9

Breach of Personal Data 10

Certification 11

Certification Bodies 12

Certification mechanisms (approved) 13

Confidentiality *(principle of)* 14

Consistency mechanism 15

Criminal convictions and offenses 16

Data concerning health 17

Data Portability *(right of)* 18

Data protection impact assessment (DPIA) 19

Data protection officer 20

Effective Judicial Remedy *(right to)* 21

Encryption 22

Erasure *(right of)* 23

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Filling System 24

Freedom of Expression and Information *(right of)* 25

Genetic data 26

Integrity and confidentiality *(principle of)* 27

Lodging a Complaint *(right of)* 28

Mutual assistance 29

Objection, object *(right to)* 30

Personal Data 31

Processing (of personal data) 33

Professional secrecy *(statutory obligation of)* 35

Protection of personal data (right to) 36

Pseudonymisation 37

Purpose limitation *(principle of)* 38

Recipient 39

Rectification *(right of)* 40

Representative of controllers or processors 41

Restriction of Processing *(right of)* 42

Storage limitation *(principle of)* 43

Third party 44

Transparency *(principle of)* or transparent 45

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Terms

Access (right of)

Definition:

A data subject should have the right of access to personal data, which have been collected and concern him or her. The data subject should be able to exercise that right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing.

More specifically, access should be provided to information regarding, primarily: the purposes for which processing has been undertaken; the categories of personal data concerned; the recipients or categories of recipients to whom the personal data have been or will be disclosed; where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing and the right to lodge a complaint with a supervisory authority.

Member States should be able to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data under certain circumstances, provided that such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned.

References: Regulation: rec 63; Art 15

Directive: rec 43-44; Arts 14, 15(1)

Example: Right of access may refer to information concerning health, for example the data in the subject's medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Accountability *(principle of)*

Definition:

Accountability is one of the principles relating to the processing of personal data, according to which the controller shall be responsible for and able to demonstrate compliance with the principles defined in article 5(1)(a)-(f) of the Regulation. More specifically with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and the principles of integrity and confidentiality.

In order to be accountable, the data controller must keep a record of its processing activities according to Art. 30 of the Regulation/Art. 24 of the Directive. Furthermore, the controller should establish and document internal policies and take measures that comply with the principles of data protection by design and data protection by default (Art. 25 of the Regulation/Art. 20 of the Directive).

Moreover, 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 ("data protection impact assessment", Art. 35 of the Regulation/Art. 27 of the Directive).

References: Regulation: rec 78, 85; Arts 5(2), 30

Directive: rec 61; Arts 4 (4), 24

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Accuracy *(principle of)*

Definition:

Accuracy is one of the principles relating to the processing of personal data. More specifically, it is expected that personal data are accurate and, where necessary, kept up to date. Furthermore, 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.

As it relates to the data subject's right to restriction of processing, this can be enacted, amongst other cases, where the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

References: Regulation: rec 39; Arts 5(1)(d), 18(1)(a)

Directive: rec 30, 32, 47; Arts 7(2), 16(3)(a)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Biometric data

Definition:

For purposes of these instruments, 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.

Biometric data constitute one of the categories of *special data*. They are by their nature particularly sensitive in relation to fundamental rights and freedoms, merit specific protection as the context of their processing could create significant risks. Processing is initially forbidden unless specifically allowed by the Regulation or Directive or stricter law of the Member State. It is also vital that processing is strictly necessary and appropriate safeguards are applied for the rights and freedoms of the data subject.

References: Regulation: rec 51, 53, 91; Arts 4.14, 9(1), 9(4)

Directive: rec 51; Arts 3.13, 10

Synonymous terms: Biometrics

Example: Facial images, dactyloscopic data

See also: Special data

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Breach of Personal Data

Definition:

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. The Regulation (Art 4.12) and Directive (Art. 3.11) define personal data breach "a breach of security" resulting ("leading to") in any "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data." Such personal data may be, or have been, "transmitted, stored or otherwise processed."

Controllers and processors are duty bound to take all suitable and required technical and organizational measures to prevent any personal data breach. In the case of a breach, the controller must notify the personal data breach to the national authority within 72 hours from having become aware of it, or else account for the reasons of their delay. This notification obligation does not apply in instances where breach "is unlikely to result in a risk to the rights and freedoms" of natural persons.

References: Regulation: rec 73, 85-88; Arts 4.12), 33(1-2), 33(3)(a), 33(3)(c)-(d), 33(5), 34(1)-(2), 34(3)(a), 34(4), 40(2)(i), 58(2)(e), 70(1)(g)-(h)

Directive: rec 61-62; Arts 3.11, 30(1)-(2), 30(3)(a), 30(3)(c)-(d), 30(5)-(6), 31(1)-(2), 31(3)(a), 31(4), 51(1)(d)-(e)

Synonymous terms: Personal Data Breach

Example: destruction of personal data, loss of personal data, alteration of personal data, unauthorised disclosure of personal data, unauthorised transfer of personal data, violation, distortion

See also: Protection of personal data; Notification of Breach

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Certification

Definition:

Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially about the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided, amongst other means, by an approved certification. The adherence of the processor to an approved certification mechanism can be used as an element to demonstrate compliance with the obligations of the controller.

The certification shall be voluntary and available via a process that is transparent. It shall be issued by the certification bodies or by the competent supervisory authority, on the basis of approved criteria, for a maximum period of three years. It may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, where the requirements for the certification are not or no longer met.

References: Regulation: rec 77, 81, 100, 166, 168; Arts 24(3), 25(3), 28(5), 28(6), 32(3), 42(1)-(8), 43(1), 43(2)(a), 43(2)(c-d), 43(3)-(9), 46(2)(f), 57(1)(n)-(q), 58(1)(c), 58(2)(h), 58(3)(e)-(f), 64(1)(c), 70(1)(n)-(q), 83(3)(j), 83(4)(b)

Synonymous terms: Authorization, Approval

See also: certification bodies; certification mechanisms

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Certification Bodies

Definition:

Certification bodies are regulated by Regulation 2016/679 in the Art. 43. They are public or private bodies with an adequate level of expertise in relation to the protection of personal data that are accredited either by the supervisory authority or the national accreditation body. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions.

The certification bodies shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. (Regulation art. 42(4)). An organization may apply for a certification or seal by providing all the necessary information and by submitting its relevant processing activities to the relevant supervisory authority or accredited certified body that oversees the relevant scheme.

All seals and certifications will be voluntary so a Data Controller or a Data Processor's obligation under the GDPR will not be reduced if they have a seal or certification, but it may go towards supporting any investigation into its GDPR compliance. Any certification or seal awarded has a maximum term of three years which can be renewed provided the Data Controller/Data Processor still meets the relevant criteria. If the criteria are not met, the certification is likely to be withdrawn.

References: Regulation: Arts 42(5-7), 43(1-2), 43(3-5), 43(7), 57(1)(p)-(q), 58(2)(h), 58(3)(e), 64(1)(c), 70(1)(o)-(q), 83(4)(b)

See also: Certification; Certification mechanisms; Supervisory authority

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Certification mechanisms (approved)

Definition:

One of the protective measures that apply to controllers or processors in relation to the cross-border transfer of personal data.

The controller or processor submits its processing to the certification mechanism in order to obtain certification. (Regulation art. 42(6)). The controller or processor shall provide the certification body, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

References: Regulation: rec 81, 100, 167-168; Arts 24(3), 25(3), 28(5), 32(3), 42(1-2), 42(6), 42(8), 43(6), 43(8-9), 46(2)(f), 57(1)(n), 70(1)(n), 83(2)(j)

Synonymous terms: controlling and approving system

See also: Certification, Certification bodies

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Confidentiality *(principle of)*

Definition:

Integrity and confidentiality are principles relating to processing of personal data that are often treated together. More specifically, it is expected that personal data is 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. This is ensured by using appropriate technical or organisational measures. Controller and processor ought to adopt and implement appropriate technical and organisational measures to that effect.

The confidentiality principle aims at the prevention of unauthorised access to or use of personal data and the equipment used for the processing. It should be ensured by the Member State's law that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. In addition, the data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

References: Regulation: rec 39, 49, 75, 83, 85, 162-163; Arts 5(1)(f), 28(3)(b), 32(1)(b), 38(5), 76

Directive: rec 28, 33, 51, 60-61, 71; Art 22(3)(b)

See also: Integrity (principle of)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Consistency mechanism

Definition:

According to the consistency mechanism, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, in order to contribute to the consistent application of the Regulation throughout the Union.

That mechanism should in particular apply where a supervisory authority intends to adopt a measure aiming to produce legal effects with regard to processing operations which substantially affect a significant number of data subjects in several Member States. The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory.

The consistency mechanism may also be used to promote a consistent application of administrative fines which the supervisory authorities maintain the power to impose in order to strengthen and harmonise administrative penalties for infringements of the Regulation.

References: Regulation: rec 81, 119, 135-136, 138, 150; Arts 28(8), 35(6), 47(1), 51(3), 60(4), 63, 66(1), 70(1)(t), 70(1)(y), 74(1)(c), 78(4)

See also: Consistent application of the regulation

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Criminal convictions and offenses

Definition:

Personal data related to criminal convictions and offenses fall within the special categories of personal data and pose a risk of varying likelihood and severity to the rights and freedoms of natural persons, likely to lead to physical, material or non-material damage. For this kind of data, a data protection impact assessment is required.

Processing of personal data relating to criminal convictions and offences shall be carried out 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.

References: Regulation: rec 75, 80, 91, 97; Arts 6(4)(c), 10, 27(2)(a), 30(5), 35(3)(b), 37(1)(c)

Directive: rec 51;

See also: security measures

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Data concerning health

Definition:

The term as defined by the 2 instruments, refers to personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. It is being listed as one of the special categories of personal data which merit higher protection and should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole.

The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures to protect the rights and freedoms of natural persons.

References: Regulation: rec 35, 53-54, 73; Arts 4.15, 9(1), 9(4)

Directive: rec 24, 51; Arts 3.14, 10

Synonymous terms: Health data, health information

Example: Data related to physical or mental health of a natural person, provision of health care services which reveal information about a person's health status, all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject, a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test. In addition, all elements related to health, health status, including morbidity and disability, the determinants influencing that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Data Portability *(right of)*

Definition:

According to data portability, the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It also includes the right of the data subject to have the personal data transmitted directly from one controller to another, where technically feasible. However, it shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Restrictions may be imposed by Union or Member State law as far as necessary and proportionate in a democratic society to safeguard public security.

The controller ought, at the time when personal data are obtained, to provide the data subject with information concerning the existence of his several rights, including the right to data portability.

References: Regulation: rec 68, 73, 156; Arts 13(2)(b), 14(2)(c), 20(2)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Data protection impact assessment (DPIA)

Definition:

Such assessment ought to be carried out by the controller prior to the processing, in cases where processing operations are likely to result in a high risk to the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing. The scope should be the evaluation of the origin, nature, particularity and severity of that risk while the outcome of the evaluation is of specific importance in determining the appropriate measures to be taken in order for the processing to comply with the Regulation and Directive.

The assessment shall contain at least a general description of the envisaged processing operations and the purposes of the processing, the legitimate interest pursued by the controller, an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the relevant legislation, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

References: Regulation: rec 84, 89-95; Arts 35, 35(2)-(5), 35(8), 35(10)-(11), 36(1), 36(3)(e), 39(1)(c), 57(1)(k), 64(1)(a)

Directive: rec 53, 58; Arts 27, 28(1)(a), 28(4), 34(c)

Example: A data protection impact assessment shall in particular be required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. In addition, in the case of processing on a large scale of special categories of data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, 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. Also in the case of personal data relating to criminal convictions and offences, or of a systematic monitoring of a publicly accessible area on a large scale. Furthermore, DPIA is needed in cases for example where processing operations may involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Data protection officer

Definition:

A data protection officer shall be designated by the controller and the processor or by a group of undertakings in particular cases such as where the processing is carried out by a public authority or body (except for courts acting in their judicial capacity). He/ She must fulfil certain professional qualities; in particular, expert knowledge of data protection law and practices, the ability to complete the tasks appointed to him by the related instruments as well as the appropriate independence, secrecy and confidentiality concerning the performance of his duties and tasks.

His/ Her tasks include informing and advising the controller or processor and their employees who carry out personal data processing of their obligations pursuant to the related legal data protection instruments of the Union and the respective Member State, monitoring compliance, awareness-raising and training of staff involved in processing operations and to provide advice where requested about the data protection impact assessment and monitor its performance.

References: Regulation: rec 77, 97; Arts 13(1)(b), 14(1)(b), 30(1)(a), 30(2)(a), 33(3)(b), 35(2), 36(3)(d), 37(1)-(7), 38(1)-(6), 39(1-2), 47(2)(h), 57(3)

Directive: rec 63; Arts 13(b), 24(1)(a), 24(2)(a), 30(2)(b), 32(1)-(4), 33(1)-(2), 34, 34(3)

Example: The data protection officer can be an existing employee of the controller or an external employee. Ideally, a data protection officer should have excellent management skills and the ability to interface easily with internal staff at all levels as well as outside authorities. He/ She must be able to ensure internal compliance and alert the authorities of non-compliance while understanding that the company may be subjected to hefty fines for non-compliance.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Effective Judicial Remedy *(right to)*

Definition:

Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person and it is believed that his or her rights under the related law are infringed. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, that right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with Member State law. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.

National law should also provide for the right of a data subject to mandate a not-for-profit body, organisation or association with statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects.

In addition, each data subject shall have the same right to an effective judicial remedy against a controller or a processor. Proceedings 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.

References: Regulation: rec 141-143; Arts 58(4), 78(1)-(2), 79(1), 79(8)

Directive: rec 85-86; Arts 47(4), 53(1)-(2), 54

See also: Lodging a complaint (right of)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Encryption

Definition:

It constitutes one of the technical and organisational measures that can be adopted by the controller or processor in order to maintain security and prevent processing in infringement of the Regulation and Directive. It assists in evaluating and mitigating the risks inherent in the processing of personal data.

It requires that the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, are taken into account.

References: Regulation: rec 83; Arts 6(4)(e), 32(1)(a), 34(3)(a)

Directive: rec 60; Art 31(3)(a)

Example: Encryption of communications (i.e. calls, online sessions, text messages), encryption by operators of critical infrastructures (ports, airports, hospitals, etc) aiming in protecting their network and information systems.

See also: pseudonymisation

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Erasure *(right of)*

Definition:

The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay in cases where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing, the data subject objects to the processing and there are no overriding legitimate grounds for the processing, the personal data have been unlawfully processed, the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject or the personal data have been collected in relation to the offer of information society services directly to a child.

The controller ought, at the time when personal data are obtained, to provide the data subject with information concerning the existence of his several rights, including the right of erasure. He also has to communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data.

References: Regulation: rec 39, 59, 66, 68, 73, 156; Arts 4.2, 13(2)(b), 14(2)(c), 15(1)(e), 17(1)-(2), 18(1)(b), 19, 30(1)(f), 58(1)(g)

Directive: rec 27, 34, 40, 42, 47-49, 57, 107; Arts 3.2, 5, 13(1)(e), 14(e), 16(2)-(4), 24(1)(h), 25(1), 47(2)(b)

See also: right to be forgotten

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Filling System

Definition:

According to the definition provided by the legislator, it means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

The personal data kept in a filing system can be either manually or electronically stored in a database.

As it relates to the restriction of processing of personal data in automated filing systems, it should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact, that the processing of personal data is restricted, should be clearly indicated in the system.

References: Regulation: rec 15, 31, 67; Arts 2(1), 4(6)

Directive: rec 18, 22, 47; Arts 2(2), 3(6), 28(1)

Example: a file concerning a competition for promotion within a workplace

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Freedom of Expression and Information *(right of)*

Definition:

The right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression, shall be reconciled with the right to personal data protection. Therefore, Member States shall work towards this direction by providing for exemptions or derogations where necessary to allow their co-existence and draw a fair balance between these fundamental rights.

Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations.

References: Regulation: rec 4, 65, 153; Arts 17(3)(a), 85(1)-(2)

Example: This right should apply in particular to the processing of personal data in the audiovisual field, and in news archives and press libraries.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Genetic data

Definition:

One of the several types of data that the EU Legislator aims to protect through Regulation 2016/679 and Directive 2016/680.

The two instruments define personal data as "relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question." (Regulation art. 4(13); Directive art. 3(12)).

It also falls into the 'special categories' of personal data for which the Regulation (art 9) and the Directive (art 10) include a special processing provision. More specifically, genetic data as well as other special categories of personal data, should be processed for health-related purposes only to the benefit of natural persons and society as a whole, or to serve the public interest, for scientific, historical research or statistical purposes.

References: Regulation: rec 34-35, 53, 75; Arts 4.13, 9(1), 9(4)

Directive: rec 23, 24, 51; Arts 3.12, 10

Synonymous terms: genetic characteristics (rec 34 and Art 13 of the Regulation, rec 23 of the Directive), genetic information (rec 23 of the Directive), genetic features (rec 23 of the Directive)

Example: The unique information about a person that consist the genetic data under protection, result from a biological sample, in particular chromosomal, DNA or RNA analysis, or from the analysis of another element enabling equivalent information to be obtained.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Integrity *(principle of)*

Definition:

Integrity and confidentiality are principles relating to processing of personal data that are often treated together. More specifically, it is to be expected that personal data be 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. This is ensured by using appropriate technical or organisational measures. Controller and processor ought to adopt and implement appropriate technical and organisational measures to that effect.

Integrity should be an important criterion assessing the adequacy and independence of a supervisory authority. It refers to the need that stored personal data cannot be corrupted by means of a malfunction of the system. Regarding the Directive, logs should be kept and used, amongst other related purposes, for ensuring data integrity and data security.

References: Regulation: rec 49, 121; Arts 5(1)(f), 32(1)(b)

Directive: rec 33, 56, 57, 79, 96; Arts 25(2), 29(2)(j)

See also: Confidentiality (principle of)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Lodging a Complaint *(right of)*

Definition:

The right to lodge a complaint derives from the right of every data subject to be informed by the controller at the time when the subject's personal data are obtained. More specifically, without prejudice to any other administrative or judicial remedy, the data subject has the right to lodge a complaint with a supervisory authority if he or she considers that the processing of their personal data infringes the relevant law. Alternatively, the data subject has the right to mandate a non-profit body, organisation or association which is constituted in accordance with the law of a respective Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf. The complaint can be lodged in the Member State of his or her habitual residence, place of work or place of the alleged infringement.

The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

References: Regulation: rec 141-142; Arts 12(4), 13(2)(d), 14(2)(e), 15(1)(f), 47(2)(e), 77(1), 79(1)

Directive: rec 42, 85, 87; Arts 13(1)(d), 14(f), 52(1), 54

See also: Effective judicial remedy (right of)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Mutual assistance

Definition:

Mutual cooperation is being approached on two different levels by the EU legislator. Firstly, at an international level, mutual cooperation for the protection of personal data is needed, more specifically, between third countries, international organisations, the Commission and supervisory authorities of the Member States. This cooperation shall aim in facilitating effective enforcement of the relevant legislation, through notification, complaint referral, investigative assistance and information exchange.

At a second level, there should be mutual assistance between supervisory authorities which ought to cooperate throughout sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of the Regulation and Directive. In addition, the same obligation exists between the lead supervisory authorities, between them and other supervisory authorities concerned as well as with the Commission. This may include the conduct of joint operations, currying out investigations or monitoring the implementation of a measure concerning a controller or processor established in another Member State.

In general, mutual assistance shall cover information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations. All appropriate measures should be taken to reply to a request of another authority without undue delay. The requested supervisory authority shall not refuse to comply with the request except under certain circumstances.

References: Regulation: rec 116, 120, 123, 133, 138, 168; Arts 50(b), 52(4), 57(1)(g), 60(2), 61(1), 61(7), 61(9), 64(2)

Directive: rec 77, 83, 90, 91, 94; Arts 40(b), 42(4), 46(1)(h), 50(1), 50(7)-(8)

Synonymous terms: International cooperation; International mutual assistance

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Objection, object *(right to)*

Definition:

The data subject retains the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her. In the case of an objection, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Restrictions concerning specific principles and rights safeguarded in the related legislation, including the right to object, may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society.

References: Regulation: rec 50, 59, 70, 73; Art 21(1)-(2), (5)-(6)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Personal Data

Definition:

Personal data are data concerning natural persons, whose protection is the main objective of the Regulation and the Directive. The two instruments define personal data as "any information relating to an identified or identifiable natural person," the *data subject*. In its turn, an *identifiable* natural person "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" (Regulation Art. 4.1; Directive Art. 3.1).

The instruments do not attempt to provide an exhaustive list of data considered as personal data for their purposes, but a demonstrative calculation of the characteristics defining the physical person is apparent. Both Regulation (Art 9) and Directive (Art 10) however do include a finite list of "special categories of personal data" – i.e. sensitive data whose processing is limited. These include: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data "for the purpose of uniquely identifying a natural person," data concerning health; and data concerning a natural person's sex life or sexual orientation.

References: Regulation: rec 1-7, 9-20, 22-24, 26-29, 31, 40, 42-43, 45-75, 78, 80-81, 83-91, 95-97, 101-105, 107-108, 110-113, 115- 117, 122-124, 127, 129, 139, 142, 153-160, 162, 164,166, 170, 173; Arts 1(1)-(3), 2(1)-(3), 3 (1)-(3), 4.1-4.16(a), 4.20, 4.22, 4.23(a)-4.23(b), 4.24), 5(1)(d)-(f), 6(1)(a), 6(1)(f), 6(3)(b), 6(4), 6(4)(a)-(c), 7(1), 7(4), 8(1), 9(1), 9(2)(a), 9(2)(d)-(e), 9(3), 10, 11(1), 13(1), 13(1)(c), 13(1)(c), 13(1)(e)-(f), 13(2), 13(2)(a)-(b), 13(2)(e), 13(3), 14(1), 14(1)(c)-(f), 14(2)(a), 14(2)(c), 14(2)(f), 14(3)(a)-(c), 14(4), 14(5)(d), 15(1), 15(1)(b)-(e), 15(1)(g), 15(2)-(3), 16, 17(1), 17(1)(a), 17(1)(d)-(f), 17(2), 18(1)(a)-(c), 18(2), 19, 20(1)-(2), 21(1)-(3), 21(6), 22(4), 23(2)(b), 25(2), 27(2)(a), 27(3), 28(3), 28(3)(a)-(b), 28(3)(g), 29, 30(1)(c)-(e), 30(2)(c), 30(5), 32(1)(a), 32(1)(c), 32(2), 32(4), 33(1)-(2), 33(3)(a), 33(3)(c)-(d), 33(5), 34(1)-(2), 34(3)(a), 34(4), 35(1), 35(2)(b), 35(6), 35(7)(d), 37(1)(c), 38(1)-(2), 38(4), 39(1)(b), 40(2)(c)-(d), 40(2)(i)-(j), 40(3), 42(2), 44, 45(1), 45(2)(a), 45(2)(c), 45(7), 46(1), 46(3)(a), 47(1)(b), 47(2)(b), 47(2)(d), 47(2)(n), 48, 49(1)-(2), 49(5), 50(a)-(d), 51(1), 53(2), 57(1)(i), 57(1)(v), 58(1)(e), 58(2)(e), 58(2)(g), 58(3)(b), 70(1)(b), 70(1)(d), 70(1)(g)-(j), 77(1), 79(1), 80(1), 83(2)(g), 83(5)(c), 85(1)-(2), 86, 88(1)-(2), 89(2)-(3), 90(1), 94(2), 96, 97(2)(a), 98

Directive: rec 1-12, 14-38, 40, 42-44, 47-51, 53, 56-58, 60-66, 68, 70-75, 80, 87, 93-95, 99-100, 104, 107; Arts 1(1), 1(2)(a)-(b), 1(3), 2(1)-(3), 3.1-3.6, 3.8-3.14, 4(1), 4(1)(d), 4(1)(f), 4(2), 4(2)(a), 5, 6, 7(1)-(3), 8(2), 9(1), 9(3), 10, 11(2)-(3), 13(1)(c), 13(1)(e), 13(2)(b)-(d), 14, 14(b)-(e), 14(g), 16(1)-(2), 16(3)(a)-(b), 16(4)-(6), 18, 20(2), 22(3),

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

22(3)(b), 22(3)(d), 23, 24(1)(c)-(d), 24(1)(f)-(h), 24(2)(c), 25(1)-(2), 27(1)-(2), 28(4), 29(1), 29(2)(c), 29(2)(e)-(h), 29(2)(j), 30(1)-(2), 30(3)(a), 30(3)(c)-(d), 30(5)-(6), 31(1)-(2), 31(3)(a), 31(4), 33(1)-(2), 34(b), 35(1), 35(1)(b)-(c), 35(1)(e), 35(2), 36(1), 36(2)(a), 36(2)(c), 36(7), 37(1), 37(1)(a)-(b), 37(3), 38(1), 38(1)(b), 38(2)-(3), 39(1), 39(1)(e), 40(a)-(d), 41(1), 43(2), 46(1)(j), 47(1), 47(2)(b), 47(3), 51(1)(a), 51(1)(d)-(e), 52(1), 54-55, 60-61, 62(2), 62(6)

Synonymous terms: - Data on physical/natural persons; personal information; information on physical/natural persons.

Example: Specific features – "identifiers" such as 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.

See also: biometric data; genetic data; data concerning health; processing of personal data

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Processing (of personal data)

Definition:

Processing of personal data is defined in both Regulation (Art. 4.2) and Directive (Art. 3.2) as "any operation or set of operations which is performed on personal data or on sets of personal data." Processing can be done by human activity or by automated means (e.g. supported by algorithm). Processing activities include "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" (Regulation Art. 4(2); Directive Art. 3(2)).

The EU legislator states that the processing of personal data "should be designed to serve mankind" (Regulation rec. 4). An essential premise of the EU data protection regime, taking account of the importance of data in modern society, is that the individual's right to the protection of personal data is not an *absolute* right, but rather a right, which must be evaluated in the light of its function in society and whose exercise and scope must be balanced against other fundamental rights, and in accordance with the principle of proportionality.

The legislator emphasizes that any processing of personal data should be lawful and fair (Regulation rec. 39). From the point of view of the controller or processor, the processing should take place only if its purpose could not reasonably be fulfilled by other means. The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. Consent of the data subject is vital. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data: this includes preventing unauthorised access to, or use, of both personal data and the equipment used for the processing of personal data. From the point of view of data subjects, these must be made aware, in accordance with the transparency principle, that personal data concerning them are or will be processed; they must be informed about the risks involved in the processing of their personal data, the rules and safeguards in place but also their rights and the ways in which to exercise such rights in relation to such processing.

References: Regulation: rec 1-4, 9-20. 22-24, 26-27, 29, 31-33, 36-40, 42-56, 58, 60-63, 65-84, 89-94, 96-98, 104-105, 108, 113-115, 117, 122-124, 126-129, 131, 135, 139, 142, 144, 146, 153-156, 158-160, 162, 171, 173; Arts 1(1), 1(3), 2(1)-(3), 3(1)-(3), 4.2-4.4., 4.7, 4.9, 4.11,

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4.14, 4.16(a)-b), 5(1)(b), 5(1)(f), 6(1), 6(1)(a)-(f), 6(2)-(4), 6(4)(a), 6(4)(d), 7(1), 7(3)-(4), 8(1), 9(1), 9(2)(a)-(j), 9(4), 10-11, 12(1), 12(7), 13(1)(c)-(d), 13(2), 13(2)(b)-(c), 13(2)(f), 13(3), 14(1)(c), 14(2), 14(2)(b)-(d), 14(2)(g), 14(4), 14(5)(b), 15(1)(a), 15(1)(e), 15(1)(h), 15(3), 16, 17(1)(b)-(c), 17(2), 17(3), 17(3)(b), 17(3)(d), 18(1), 18(1)(b)-(d), 18(2)-(3), 19, 20(1)(a)-(b), 20(3), 21(1)-(3), 21(6), 22(1), 23(2)(a), 23(2)(f), 24(1)-(2), 25(1)-(2), 26(1), 27(2)(a), 27(4), 28(1), 28(3), 28(3)(a), 28(3)(e)-(g), 28(4), 28(10), 29, 30(1)(b), 30(2), 30(2)(b), 30(5), 32(1), 32( )(b), 32(1)(d), 32(2), 35(1), 35(3)(a)-(b), 35(4)-(6), 35(7)(a)-(b), 35(8)-(11), 36(1)-(2), 36(2)(a)-(b), 36(4)-(5), 37(1)(a)-(c), 38(2), 38(4), 39(1)(a)-(b), 39(1)(e), 39(2), 40(1), 40(2)(a), 40(2)(h), 40(2)(k), 40(6), 41(6), 42(1), 42(6), 44, 47(1)(b), 47(2)(b), 47(2)(d)-(e), 51(1), 55(2)-(3), 56(1), 56(6), 57(1)(b)-(c), 57(1)(l), 58(1)(f), 58(2)(a)-(b), 58(2)(d), 58(2)(f)-(g), 58(3)(c), 60(10), 62(2), 64(1)(a), 71(1), 77(1), 79(1), 80(2), 81(1)-(2), 82(2), 82(4)-(5), 83(2)(a), 83(3), 83(5)(a), 83(5)(e), 85(1)-(2), 86-87, 88(1)-(2), 89(1), 89(4), 91(1), 94(2), 95, 98,

Directive: rec 1-2, 5-9, 11-12, 14-15, 17-22, 25-26, 28-31, 33-38, 40, 42-43, 47-61, 63, 67-68, 73, 75, 80, 88, 94, 96, 99-100, 107; Arts 1(1), 1(2)(b), 1(3), 2(1)-(3), 3.2-3.5, 3.8, 3.10, 3.13, 4(1)(f), 4(2), 4(2)(b), 4(3), 7(3), 8(1)-(2), 9(1)-(3), 10, 10(c), 11(1), 12(1), 13(1)(c), 13(1)(e), 13(2)(a), 13(4), 14(a), 14(e), 14(g), 15(2), 16(1)-(4), 16(6), 19(1)-(2), 20(1)-(2), 21(1), 22(1), 22(3), 22(3)d), 22(5), 23, 24(1), 24(1)(b), 24(1)(g), 24(2), 24(2)(b), 25(1)-(2), 27(1)-(2), 28(1), 28(1)(a)-(b), 28(2)-(5), 29(1)-(2), 29(2)(a), 29(2)(d)-(e), 29(2)(g), 33(2), 34(a)-(b), 34(e), 35(1), 39(1)(e), 41(1), 45(2), 46(1)(b)-(c), 46(1)(g), 46(1)(k), 47(2)(a)-(c), 51(1), 52(1), 54, 56, 60, 62(6), 63(2)-(3)

Synonymous terms: elaboration, manipulation, data handling, organising

Example: collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure, destruction

See also: Restriction of processing; transparency principle; protection of data subject; freedom of expression and information (right of); purpose limitation (principle of)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Professional secrecy *(statutory obligation of)*

Definition:

Professional secrecy constitutes one of the situations which, when fulfilled, allows the otherwise forbidden processing of special categories of personal data (such as 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). Therefore, processing can take place where it is necessary for 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, given that the Union or Member State law provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

It is also important that the member or members and the staff of each supervisory authority be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers.

References: Regulation: rec 53, 75, 85, 164; art 9(2)(i), 9(3), 14(5)(d), 54(2), 90(1)

Directive: rec 51, 61; art 44(2)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Protection of personal data (right to)

Definition:

The effective protection of personal data throughout the Union is a stated EU legislative policy, whose implementation requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

This is the main objective of the Regulation and the Directive (see especially Art. 1(2) and 1(1) respectively). Even though neither instrument contains an express definition of what constitutes protection of personal data, both instruments go at great length to define personal data, to regulate processing of personal data, to state the rights of data subjects and to prescribe both preventive mechanisms and appropriate remedies in case of breach. Protection of personal data is moreover a statutory undertaking (express commitment) for the various processing bodies. Finally, controllers are required to ensure the protection of personal data by security measures and mechanisms.

The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to protection of their own personal data. It is however not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights (such as respect for private and family life, home and communications; freedom of thought, conscience and religion; freedom of expression and information; freedom to conduct a business; right to an effective remedy and to a fair trial; cultural, religious and linguistic diversity), in accordance with the principle of proportionality.

References: Regulation: rec 1-2, 4, 6, 9, 11, 89-90, 101, 105, 116, 129, 142, 153-154, 164, 166; Arts 1(2), 6(1)(f), 35(1), 35(7)(d), 38(1), 39(1)(b), 45(2)(c), 49(1), 50(1(a)-c)), 53(2), 57(1)(i), 57(1)(v), 58(3)(b), 70(1)(b), 70(1)(i), 85(1-2), 86, 90(1), 98,

Directive: rec 1-4, 7, 10, 16, 58, 68, 71, 93-95, 104; art 1(2)(a), 27(1-2), 28(4), 33(1), 34(b), 36(2)(c), 37(1)(a)-(b), 40(a)-(c), 43(2), 46(1)(j), 47(3), 51(1)(a), 60, 62(6),

Synonymous terms: Personal data protection rights

See also: breach of personal data; Data Protection Officer; effective judicial remedy (right to); erasure (right to); supervisory authority; processing of personal data; rectification (right of); transparency (principle of)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Pseudonymisation

Definition:

Both new legal instruments on personal data protection define Pseudonymisation as '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'.

It constitutes one of the safeguards that should be adopted in order to secure the lawfulness of any proceedings related to the processing of personal data of any identified or identifiable natural person. The EU legislator underlines that such a measure should be activated as early as possible in the processing procedure.

The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors meet their data-protection obligations. It can also serve as a tool that could facilitate, in particular, the free flow of personal data within the area of freedom, security and justice. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

References: Regulation: rec 26, 28-29, 75, 85, 156; Arts 4.5, 6(4)(e), 25(1), 32(1)(a), 40(2)(d), 89(1)

Directive: rec 51, 53, 61; Arts 3.5, 20(1)

See also: encryption

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Purpose limitation *(principle of)*

Definition:

Purpose limitation, is one of the principles relating to the processing of personal data. More specifically, personal data shall be 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 not be considered to be incompatible with the initial purposes, provided that Member States ensure appropriate safeguards.

There should be a legal basis either at a Union or Member State level that will establish specifications for determining several aspects of the processing, including the purpose limitations.

References: Regulation: rec 39, 45, 50; Arts 5(1)(b), 6(3), 47(2)(d)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Recipient

Definition:

As defined by the legislator, recipient is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law (such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets), shall not be regarded as recipients; the processing of the specific data by those authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

The data subject ought to be informed about the recipient or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients established in third countries or international organisations.

References: Regulation: rec 31, 61, 63, 101, 111; art 4.9, 13(1)(e), 14(1)(e)-(f), 14(3)(c), 15(1)(c), 19, 30(1)(d), 46(3)(a), 49(2), 58(2)(g), 58(2)(j), 83(5)(c)

Directive: rec 22, 34, 36, 43, 47, 64, 73; Arts 3.10, 7(3), 9(3)-(4), 13(2)(c), 14(c), 16(6), 24(1)(c), 25(1), 39(1), 39(1)(c)

Synonymous terms: addressee, receiver

Example: controller, processor, employer, insurance company, bank

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Rectification *(right of)*

Definition:

It constitutes a right of every data subject for which he ought to be informed by the controller at the time when the personal data are obtained. It allows the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. It includes, having the purposes of the processing taken into account, the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Where the controller denies a data subject his or her right to rectification of personal data, the data subject should have the right to request to the national supervisory authority to verify the lawfulness of the processing.

Restrictions concerning specific principles and rights safeguarded in the related legislation, including the right of rectification, may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society.

References: Regulation: rec 59, 73, 156; art 13(2)(b), 14(2)(c), 15(1)(e), 16, 19, 58(2)(g)

Directive: rec 40, 42, 47-49, 107; art 13(1)(e), 14(e), 16(1), 16(4)-(5), 47(2)(b)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Representative of controllers or processors

Definition:

According to the legislator, representative means a natural or legal person established in the Union who represents the controller or processor with regard to their respective obligations under this Regulation. He/ She is designated by the controller or processor in writing, without however affecting the responsibility or liability of the controller or the processor under the Regulation.

Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union in relation to the offering of goods or services, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, a representative should be designated.

In general, the representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. Such a representative should perform his/ her tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. He/ She should be subject to enforcement proceedings in an event of non-compliance by the controller or processor.

References: Regulation: rec 80, 139; art 4.17, 13(1)(a), 14(1)(a), 27, 27(1), 27(3)-(5), 30(1), 30(1)(a), 30(2), 30(2)(a), 30(4), 31, 35(9), 58(1)(a), 68(3)-(5), 76(2)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Restriction of Processing *(right of)*

Definition:

According to the legislator, restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future. It constitutes a right of every data subject to be informed by the controller at the time when the personal data is obtained.

More specifically, the data subject shall have the right to obtain from the controller restriction of processing in specific cases. These are cases where the accuracy of the personal data is contested by the data subject for a period enabling the controller to verify the accuracy of the personal data, where the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; where the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; and where the data subject has exercised his/ her right to object to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of great public interest of the Union or of a Member State.

References: Regulation: rec 67, 156; Arts 4.3, 13(2)(b), 14(2)(c), 15(1)(e), 18(1), 18(3), 19, 58(2)(g)

Directive: rec 34, 40, 42, 47-49, 107; Arts 3.3, 13(1)(e), 14(e), 16(3-4), 47(2)(b)

Example: Methods by which to restrict the processing of personal data could include temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Storage limitation *(principle of)*

Definition:

Storage limitation is one of the principles related to the processing of personal data. More specifically, personal data shall be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in public interest, scientific or historical research purposes, or statistical purpose, subject to measures safeguarding the rights and freedoms of the data subject.

References: Regulation: rec 39, 45; art 5(1)(e), 6(3), 13(2)(a), 14(2)(a), 15(1)(d), 23(2)(f), 25(2), 47(2)(d)

Directive: rec 26, 41, 42; Arts 4(1(e)), 5, 13(2)(b), 14(d), 20(2)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Third party

Definition:

For the purposes of the Regulation and the Directive, third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

The legitimate interests of such a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding.

References: Regulation: rec 47, 69; Arts 4.9, 4.10, 6(1)(f), 13(1)(d), 14(2)(b)

Directive: rec 10

Example: employer, insurance company, bank

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Transparency *(principle of)* or transparent

Definition:

Transparency is a principle related to the processing of personal data. It should be transparent to natural persons that their personal data are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The specific purposes for which personal data are processed should be explicit, legitimate and determined at the time of the collection of the personal data. It is additionally required that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, using a clear and plain language. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data, and of how to exercise their rights in relation to such a processing. These are obligations of the data controller.

Such information could be provided in electronic form, for example, when addressed to the public, through a website. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

References: Regulation: rec 13, 39, 58, 60, 71, 78, 100, 121; Arts 5(1)(a), 12(1), 13(2), 14(2), 26(1), 40(2)(a), 41(2)(c), 42(3), 43(2)(d), 53(1), 88(2)

Directive: rec 26, 79; Arts 21(1), 43(1)

Example: Such information necessary to ensure fair and transparent processing are the period for which the personal data will be stored, the existence of the right to request from the controller access to, and rectification or erasure of personal data, or restriction of processing concerning the data subject, or to object to processing as well as the right to data portability, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, the right to lodge a complaint with a supervisory authority, whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data, the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.