

**Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
(COM(2012)0011 – C7 0025/2012 – 2012/0011(COD))**

Compromise amendements on Articles 1-29

**COMP Article 1
07.10.2013**

**CHAPTER I
GENERAL PROVISIONS**

**Article 1
Subject matter and objectives**

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

Recitals

(1) 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 lay down that everyone has the right to the protection of personal data concerning him or her.

(2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of individuals.

(3) 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 data¹ seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.

(4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between economic and social, public and private actors across the Union increased. National authorities in the Member States are being called upon by Union law to co-operate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring an high level of the protection of personal data.

(6) These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance to create the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.

(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of

¹ OJ L 281, 23.11.1995, p. 31.

the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.

(9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.

(10) Article 16(2) of the Treaty mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.

In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

(11) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the legal person contains the names of one or more natural persons.

(12) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.

COMP Article 2

7.10.2013

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means, *irrespective of the method of processing*, 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.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law, ~~*in particular national security*~~;

~~*(b) by the Union institutions, bodies, offices and agencies;*~~

(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of *Title V* of the Treaty on European Union;

(d) by a natural person ~~*without any gainful interest*~~ in the course of ~~*its own*~~ an exclusively personal or household activity. *This exemption also shall apply to a publication of personal data where it can be reasonably expected that it will be only accessed by a limited number of persons;*

(e) by competent *public* authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Recitals

(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, ~~*nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies, which are subject to Regulation (EC) No 45/2001, or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union. Regulation (EC) No 45/2001 should be brought in line with this Regulation and applied in accordance with this Regulation.*~~

(15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal, *family-related*, or domestic, such as correspondence and the holding of addresses *or a private sale* and without any connection with a professional or commercial activity. *However, this Regulation should apply to controllers and processors which provide the means for processing personal data for such personal or domestic activities.*

COMP Article 3

14.10.2013

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, ***whether the processing takes place in the Union or not.***

2. This Regulation applies to the processing of personal data of data subjects ~~residing~~ in the Union by a controller ***or processor*** not established in the Union, where the processing activities are related to:

(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; or

(b) the monitoring of ***such data subjects their behaviour.***

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

Recitals

(19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services, ***irrespective of whether connected to a payment or not,*** to such data subjects, or to the monitoring ~~of the behaviour~~ of such data subjects. ***In order to determine whether such a controller is offering goods or services to such data subjects in the Union, it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects residing in one or more Member States in the Union.***

(21) In order to determine whether a processing activity can be considered to ‘monitor’ ~~the behaviour~~ of data subjects, it should be ascertained whether individuals are tracked,

regardless of the origins of the data ~~on the internet with or through other means~~, or if other data about them is collected, including from public registers and announcements in the Union that are accessible from outside of the Union, including with the intention to use, or potential of subsequent use of data processing techniques which consist of applying a 'profile' ~~to an individual~~, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

COMP Article 4

11.10.2013

Article 4

Definitions

For the purposes of this Regulation:

~~(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;~~

(2) 'personal data' means 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 identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person;*

(2a) '*pseudonymous data*' means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution;

(2b) '*encrypted data*' means personal data, which through technological protection measures is rendered unintelligible to any person who is not authorised to access it;

(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;

(3a) '*profiling*' means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour;

(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, ~~conditions~~ and means of the processing of personal data; where the purposes, ~~conditions~~ and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;

(7a) 'third party' means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

(9) 'personal data breach' means ~~a breach of security leading to~~ the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(10) 'genetic data' means all ***personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained;***

(11) 'biometric data' means any ***personal*** data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;

(12) 'data concerning health' means any ***personal data information*** which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

(13) 'main establishment' means the place of establishment of the undertaking or group of undertakings in the Union, whether controller or processor, where the main decisions as to the purposes, conditions and means of the processing of personal data are taken. The following objective criteria may be considered among others: The location of the controller or processor's headquarters; the location of the entity within

a group of undertakings which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; the location where effective and real management activities are exercised determining the data processing through stable arrangements;

(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, ~~acts and may be addressed by the supervisory authority and other bodies in the Union instead of the~~ *represents the* controller, with regard to the obligations of the controller under this Regulation;

(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;

(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;

(18) 'child' means any person below the age of 18 years;

(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.

Recitals

(23) The principles of *data* protection should apply to any information concerning an identified or identifiable *natural* person. *To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes.*

(24) When using ~~online services, individuals may be associated with online~~ identifiers provided by ~~their~~ devices, applications, tools and protocols, such as Internet Protocol addresses, cookie identifiers *and Radio Frequency Identification tags, this Regulation*

should be applicable to processing involving such data, unless those identifiers do not relate to an identified or identifiable natural person. ~~This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.~~

(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action ***that is the result of choice*** by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data. ***Clear affirmative action could include*** ~~including~~ by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence, ***mere use of a service*** or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

COMP Article 5
07.10.2013

Article 5
Principles relating to personal data processing

Personal data ~~must~~ *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 way incompatible with those purposes (*purpose limitation*);

(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data (*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 *direct or indirect* 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 data will be processed solely for historical, statistical or scientific research *or for archive* purposes in accordance with the rules and conditions of Articles 83 *and 83a* and if a periodic review is carried out to assess the necessity to continue the storage, *and if appropriate technical and organisational measures are put in place to limit access to the data only for these purposes (storage minimisation)*;

(ea) processed in a way that effectively allows the data subject to exercise his or her rights (effectiveness);

(eb) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity);

(f) processed under the responsibility and liability of the controller, who shall ensure and *be able to* demonstrate ~~for each processing operation~~ the compliance with the provisions of this Regulation (*accountability*).

Recitals

(30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes. ***This should also mean that personal data are processed in a way that effectively allows the data subject to exercise his or her rights.***

COMP Article 6 16.10.2013

Article 6 Lawfulness of processing

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) 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;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by *the controller or in case of disclosure, by the third party to whom the data is disclosed, and which meet the reasonable expectations of the data subject based on his or her relationship with the controller*, 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~~. This shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law, or

(b) law of the Member State to which the controller is subject.

The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to

the protection of personal data and be proportionate to the legitimate aim pursued. *Within the limits of this Regulation, the law of the Member State may provide details of the lawfulness of processing, particularly as regards data controllers, the purpose of processing and purpose limitation, the nature of the data and the data subjects, processing measures and procedures, recipients, and the duration of storage.*

~~4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.~~

~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraphs 1a to 1c for various sectors and data processing situations, including as regards the processing of personal data related to a child.~~

Recitals

(35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.

(36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. *This should include also collective agreements that could be recognised under national law as having general validity.* It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.

(37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life.

(38) The legitimate interests of *the a* controller, *or in case of disclosure, by the third party to whom the data is disclosed,* may provide a legal basis for processing, provided *that they meet the reasonable expectations of the data subject based on his or her relationship with the controller and* that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. *Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, processing limited to pseudonymous data should be presumed to meet the reasonable expectations of the data subject based on his or her*

relationship with the controller. The data subject should have the right to object the processing, ~~on grounds relating to their particular situation and~~ free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. ***The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.*** Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.

(39) The processing of data to the extent strictly necessary ***and proportionate*** for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, ~~at a given level of confidence,~~ accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems. ***This principle also applies to processing of personal data to restrict abusive access to and use of publicly available network or information systems, such as the blacklisting of electronic identifiers.***

(39a) Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, the prevention or limitation of damages on the side of the data controller should be presumed as carried out for the legitimate interest of the data controller or in case of disclosure, by the third party to whom the data is disclosed, and as meeting the reasonable expectations of the data subject based on his or her relationship with the controller. The same principle also applies to the enforcement of legal claims against a data subject, such as debt collection or civil damages and remedies.

(39b) Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, the processing of personal data for the purpose of direct marketing for own or similar products and services or for the purpose of postal direct marketing should be presumed as carried out for the legitimate interest of the controller, or in case of disclosure, of the third party to whom the data is disclosed, and as meeting the reasonable expectations of the data subject based on his or her relationship with the controller if highly visible information on the right to object and on the source of the personal data is given. The processing of business contact details should be generally regarded as carried out for the legitimate interest of the controller, or in case of disclosure, of the third party to whom the data is disclosed, and as meeting

the reasonable expectations of the data subject based on his or her relationship with the controller. The same should apply to the processing of personal data made manifestly public by the data subject.

~~*(40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.*~~

COMP Article 7

14.10.2013

Article 7

Conditions for Consent

1. *Where processing is based on consent*, the controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.

2. If the data subject's consent is given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented *clearly distinguishable* in its appearance from this other matter. *Provisions on the data subject's consent which are partly in violation of this Regulation are fully void.*

3. *Notwithstanding other legal grounds for processing*, the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. *It shall be as easy to withdraw consent as to give it. The data subject shall be informed by the controller if withdrawal of consent may result in the termination of the services provided or of the relationship with the controller.*

~~4. Consent shall not provide a legal basis for the processing, where there is a significant, imbalance between the position of the data subject and the controller. Consent shall be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected. The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1), point (b).~~

Recitals

(31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation. *In case of a child or a person lacking legal capacity, relevant Union or Member State law should determine the conditions under which consent is given or authorised by that person.*

(32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given. *To comply with the principle of data minimisation, the burden of proof should*

not be understood as requiring the positive identification of data subjects unless necessary. Similar to civil law terms (Directive 93/13/EEC), data protection policies should be as clear and transparent as possible. They should not contain hidden or disadvantageous clauses. Consent can not be given for the processing of personal data of third persons.

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment. *This is especially the case if the controller is a public authority that can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given. The use of default options which the data subject is required to modify to object to the processing, such as pre-ticked boxes, does not express free consent. Consent for the processing of additional personal data that are not necessary for the provision of a service should not be a required for using the service. When consent is withdrawn, this may allow the termination or non-execution of a service which is dependent on the data. Where the conclusion of the intended purpose is unclear, the controller should in regular intervals provide the data subject with information about the processing and request a re-affirmation of their consent.*

~~(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.~~

COMP Article 8
11.10.2013

Article 8
Processing of personal data of a child

1. For the purposes of this Regulation, in relation to the offering of ~~information society goods or~~ services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or ~~custodian~~ **legal guardian**. The controller shall make reasonable efforts to ~~verify such obtain verifiable~~ consent, taking into consideration available technology ~~without causing otherwise unnecessary processing of personal data~~.

1a. Information provided to children, parents and legal guardians in order to express consent, including about the controller's collection and use of personal data, should be given in a clear language appropriate to the intended audience.

2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

3. The ~~European Data Protection Board Commission~~ shall be *entrusted with the task empowered to adopt delegated acts in accordance with Article 86 for the purpose of issuing guidelines, recommendations and best practices further specifying the criteria and requirements* for the methods of ~~verifying to obtain verifiable~~ consent referred to in paragraph 1, *in accordance with Article 66*.

~~4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

Recitals

(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. ~~To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child. Where data processing is based on the data subject's consent in relation to the offering of goods or services directly to a child, consent should be given or authorised by the child's parent or legal guardian in cases where the child is below the age of 13. Age-appropriate language should be used where the intended audience is children. Other grounds of lawful processing such as grounds of public interest should remain applicable, such as for processing in the context of preventive or counselling services offered directly to a child.~~

COMP Article 9
15.10.2013

Article 9
Special categories of data

1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or *philosophical* beliefs, *sexual orientation or gender identity*, trade-union membership *and activities*, and the processing of genetic *or biometric* data or data concerning health or sex life, ~~or~~ *administrative sanctions, judgments*, criminal *or suspected offences*, convictions, or related security measures shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given consent to the processing of those personal data *for one or more specified purposes*, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject, or

(aa) processing is necessary for the performance or execution 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;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law *or collective agreements* providing for adequate safeguards *for the fundamental rights and the interests of the data subject such as right to non-discrimination, subject to the conditions and safeguards referred to in Article 82*; or

(c) 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 consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards 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 or to former 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 outside that body without the consent of the data subjects;

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

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

(g) processing is necessary for the performance of a task carried out ~~in the~~ *for reasons of high public interest*, on the basis of Union law, 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 measures to safeguard the fundamental rights and the data subject's legitimate interests of the data subject*; or

(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or

(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or

(i a) processing is necessary for archive services subject to the conditions and safeguards referred to in Article 83a; or

(j) processing of data relating to *administrative sanctions, judgments, criminal offences, convictions or related security measures* is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards *for the fundamental rights and the interests of the data subject*. ~~A complete~~ Any register of criminal convictions shall be kept only under the control of official authority.

3. The *European Data Protection Board Commission* shall be *entrusted with the task empowered to adopt delegated acts in accordance with Article 86 for the purpose of issuing guidelines, recommendations and best practices further specifying the criteria and requirements* for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2, *in accordance with Article 66*.

Recitals

~~(41) Personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.~~

(42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the

management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, ~~or~~ for historical, statistical and scientific research purposes, ***or for archive services.***

COMP Article 10
11.10.2013

Article 10

Processing not allowing identification

*1. If the data processed by a controller do not permit the controller **or processor** to **directly or indirectly** identify a natural person, **or consist only of pseudonymous data**, the controller shall not ~~be obliged to process or~~ acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.*

2. Where the data controller is unable to comply with a provision of this Regulation because of paragraph 1, the controller shall not be obliged to comply with that particular provision of this Regulation. Where as a consequence the data controller is unable to comply with a request of the data subject, it shall inform the data subject accordingly.

Recitals

(45) If the data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. In case of a request for access, the controller should be entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks. *If it is possible for the data subject to provide such data, controllers should not be able to invoke a lack of information to refuse an access request.*

COMP Article 10a

7.10.2013

Article 10a

General principles for data subject rights

1. The basis of data protection is clear and unambiguous rights for the data subject which shall be respected by the data controller. The provisions of this Regulation aim to strengthen, clarify, guarantee and where appropriate, codify these rights.

2. Such rights include, inter alia, the provision of clear and easily understandable information regarding the processing of his or her personal data, the right of access, rectification and erasure of their data, the right to obtain data, the right to object to profiling, the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as the right to compensation and damages resulting from an unlawful processing operation. Such rights shall in general be exercised free of charge. The data controller shall respond to requests from the data subject within a reasonable period of time.

COMP Article 11

7.10.2013

Article 11

Transparent information and communication

1. The controller shall have *concise*, transparent, *clear* and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.

2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, ~~*adapted to the data subject*~~, in particular for any information addressed specifically to a child.

Recitals

(46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand.

COMP Article 12

11.10.2013

Article 12

Procedures and mechanisms for exercising the rights of the data subject

~~1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19.~~ Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically *where possible*.

2. The controller shall inform the data subject without *undue* delay and, at the latest within ~~one month~~ *40 calendar days* of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing *and, where possible, the data controller may provide remote access to a secure system which would provide the data subject with direct access to their personal data*. Where the data subject makes the request in electronic form, the information shall be provided in electronic form *where possible*, unless otherwise requested by the data subject.

3. If the controller ~~does not refuse to~~ take action on the request of the data subject, the controller shall inform the data subject of the reasons for the *inaction refusal* and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a *reasonable fee taking into account the administrative costs* for providing the information or ~~the controller may not take~~ taking the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

~~5. The Commission shall be empowered to adopt, delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.~~

~~6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and~~

~~*medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Recitals

(47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to **request obtain**, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a **reasonable** deadline and give reasons, in case he does not comply with the data subject's request.

COMP Article 13

7.10.2013

Article 13

~~Rights in relation to recipients~~

Notification requirement in the event of rectification and erasure

The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been *transferred disclosed*, unless this proves impossible or involves a disproportionate effort. *The controller shall inform the data subject about those recipients if the data subject requests this.*

COMP Article 13a
14.10.2013

Article 13a (new)
Standardised information policies

1) Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following particulars before providing information pursuant to Article 14:

- a) whether personal data are collected beyond the minimum necessary for each specific purpose of the processing;***
- b) whether personal data are retained beyond the minimum necessary for each specific purpose of the processing;***
- c) whether personal data are processed for purposes other than the purposes for which they were collected;***
- d) whether personal data are disseminated to commercial third parties;***
- e) whether personal data are sold or rented out;***
- f) whether personal data are retained in encrypted form.***

2) The particulars referred to in paragraph 1 shall be presented pursuant to Annex X in an aligned tabular format, using text and symbols, in the following three columns:
a) the first column depicts graphical forms symbolising those particulars;
b) the second column contains essential information describing those particulars;
c) the third column depicts graphical forms indicating whether a specific particular is met.

3) The information referred to in paragraphs 1 and 2 shall be presented in an easily visible and clearly legible way and shall appear in a language easily understood by the consumers of the Member States to whom the information is provided. Where the particulars are presented electronically, they shall be machine readable.

4) Additional particulars shall not be provided. Detailed explanations or further remarks regarding the particulars referred to in paragraph 1 may be provided together with the other information requirements pursuant to Article 14.

5) The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86 for the purpose of further specifying the particulars referred to in paragraph 1 and their presentation as referred to in paragraph 2 and in Annex 1.

Annex 1 - Presentation of the particulars referred to in Article 13a (new)

1) Having regard to the proportions referred to in point 6, particulars shall be provided as follows:

ICON	ESSENTIAL INFORMATION	FULFILLED
	<p>No personal data are collected beyond the minimum necessary for each specific purpose of the processing</p>	
	<p>No personal data are retained beyond the minimum necessary for each specific purpose of the processing</p>	
	<p>No personal data are processed for purposes other than the purposes for which they were collected</p>	
	<p>No personal data are disseminated to commercial third parties</p>	
	<p>No personal data are sold or rented out</p>	
	<p>No personal data are retained in unencrypted form</p>	

2) *The following words in the rows in the second column of the table in point 1, entitled "ESSENTIAL INFORMATION", shall be formatted as bold:*

- a) the word "collected" in the first row of the second column;*
- b) the word "retained" in the second row of the second column;*
- c) the word "processed" in the third row of the second column;*
- d) the word "sold and rented out" in the fifth row of the second column;*
- e) the word "disseminated" in the fourth row of the second column;*
- f) the word "unencrypted" in the sixth row of the second column.*

3) *Having regard to the proportions referred to in point 6, the rows in the third column of the table in point 1, entitled "FULFILLED", shall be completed with one of the following two graphical forms in accordance with the conditions laid down under point 4:*

a)



b)



4)

a) If no personal data are collected beyond the minimum necessary for each specific purpose of the processing, the first row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

b) If personal data are collected beyond the minimum necessary for each specific purpose of the processing, the first row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

c) If no personal data are retained beyond the minimum necessary for each specific purpose of the processing, the second row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

d) If personal data are retained beyond the minimum necessary for each specific purpose of the processing, the second row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

e) If no personal data are processed for purposes other than the purposes for which they were collected, the third row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

f) If personal data are processed for purposes other than the purposes for which they were collected, the third row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

g) If no personal data are disseminated to commercial third parties, the fourth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

h) If personal data are disseminated to commercial third parties, the fourth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

i) If no personal data are sold or rented out, the fifth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

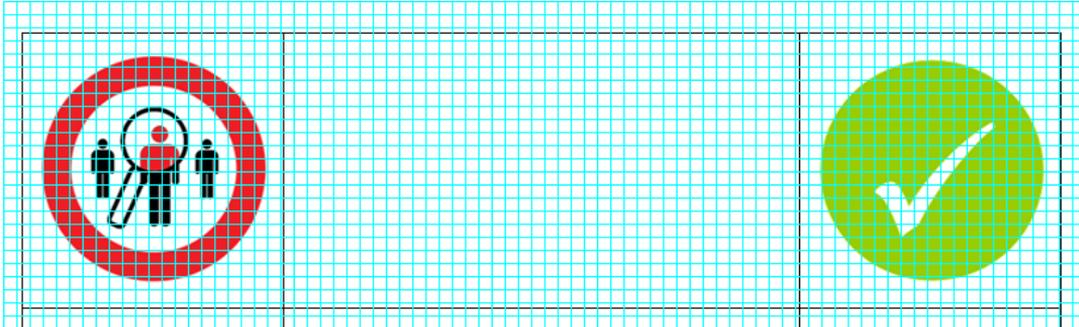
j) If personal data are sold or rented out, the fifth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

k) If no personal data are retained in unencrypted form, the sixth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3a.

l) If personal data are retained in unencrypted form, the sixth row of the third column of the table in point 1 shall entail the graphical form referred to in point 3b.

5) The reference colours of the graphical forms in point 1 in Pantone are Black Pantone No 7547 and Red Pantone No 485. The reference colour of the graphical form in point 3a in Pantone is Green Pantone No 370. The reference colour of the graphical form in point 3b in Pantone is Red Pantone No 485.

6) *The proportions given in the following graduated drawing shall be respected, even where the table is reduced or enlarged:*



COMP Article 14
17.10.2013

Article 14
Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information, *after the particulars pursuant to Article 13a have been provided*:

(a) the identity and the contact details of the controller and, if any, of the controller's representative, of the data protection officer;

(b) the purposes of the processing for which the personal data are intended, *as well as information regarding the security of the processing of personal data*, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and ~~the legitimate interests pursued by the controller, where applicable, information on how they implement and meet the requirements of point f of Article 6(1)~~;

(c) the period for which the personal data will be stored, *or if this is not possible, the criteria used to determine this period*;

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject to object to the processing of such personal data, *or to obtain data*;

(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(f) the recipients or categories of recipients of the personal data;

(g) where applicable, that the controller intends to transfer *the data* to a third country or international organisation and on ~~the level of protection afforded by that third country or international organisation by reference to the existence or absence of~~ an adequacy decision by the Commission, *or in case of transfers referred to in Article 42, Article 43, or point (h) of Article 44(1), reference to the appropriate safeguards and the means to obtain a copy of them*;

(ga) where applicable, information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject;

(gb) meaningful information about the logic involved in any automated processing;

(h) any further information **which is** necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected **or processed, in particular the existence of certain processing activities and operations for which a personal data impact assessment has indicated that there may be a high risk;**

(ha) where applicable, information whether personal data was provided to public authorities during the last consecutive 12-month period.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is **obligatory mandatory** or **voluntary optional**, as well as the possible consequences of failure to provide such data.

2a. In deciding on further information which is necessary to make the processing fair under 1(h), controllers shall have regard to any relevant guidance under Article 38.

3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the **specific** personal data originate. **If personal data originates from publicly available sources, a general indication may be given.**

4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:

(a) at the time when the personal data are obtained from the data subject **or without undue delay where the above is not feasible;** or

(aa) on request by a body, organization or association referred to in Article 73;

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a **disclosure transfer** to another recipient is envisaged, and at the latest ~~when the data are first disclosed~~ **at the time of the first transfer, or, if the data are to be used for communication with the data subject concerned, at the latest at the time of the first communication to that data subject;** or

(bb) only on request where the data are processed by a small or micro enterprise which processes personal data only as an ancillary activity.

5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or

(b) the data **are processed for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Articles 81 and 83,** are not

collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort *and the controller has published the information for anyone to retrieve*; or

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law *to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests, considering the risks represented by the processing and the nature of the personal data*; or

(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others *natural persons*, as defined in Union law or Member State law in accordance with Article 21.

(da) the data are processed in the exercise of his profession by, or are entrusted or become known to, a person who is subject to an obligation of professional secrecy regulated by Union or Member State law or to a statutory obligation of secrecy, unless the data is collected directly from the data subject.

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's *rights or* legitimate interests.

~~7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises.~~

~~8. The Commission shall lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary as well as the needs of the relevant stakeholders. Those implementing acts shall be adopted, after requesting an opinion of the European Protection Board, in accordance with the examination procedure referred to in Article 87(2).~~

Recitals

(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be *likely stored for each purpose, if the data are to be transferred to third parties or third countries*, on the existence *of measures to object and* of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they

are obliged to provide the data and of the consequences, in cases they do not provide such data. ***This information should be provided, which can also mean made readily available, to the data subject after the provision of simplified information in the form of standardised icons.***

(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.

(50) However, it is not necessary to impose this obligation where the data subject already ~~***disposes of***~~ ***knows*** this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. ~~***The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.***~~

COMP Article 15 and 18

16.10.2013

Article 15

Right to access and to obtain data for the data subject

1. *Subject to Article 12(4)*, the data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed, *and in clear and plain language*, the following information:

- (a) the purposes of the processing *for each category of personal data*;
- (b) the categories of personal data concerned;
- (c) the recipients ~~*or categories of recipients*~~ to whom the personal data are to be or have been disclosed, *in particular including* to recipients in third countries;
- (d) the period for which the personal data will be stored, *or if this is not possible, the criteria used to determine this period*;
- (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;
- (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
- ~~(g) communication of the personal data undergoing processing and of any available information as to their source;~~
- (h) the significance and envisaged consequences of such processing, ~~*at least in the case of measures referred to in Article 20.*~~
- (ha) meaningful information about the logic involved in any automated processing;*
- (hb) without prejudice to Article 21, in the event of disclosure of personal data to a public authority as a result of a public authority request, confirmation of the fact that such a request has been made.*

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in *an* electronic *and structured* format, unless otherwise requested by the data subject. *Without prejudice to Article 10, the*

controller shall take all reasonable steps to verify that the person requesting access to the data is the data subject.

2a. Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.

2b. This Article shall be without prejudice to the obligation to delete data when no longer necessary under Article 5(1)(e).

2c. There shall be no right of access in accordance with paragraphs 1 and 2 when data within the meaning of Article 14(5)(da) are concerned, except if the data subject is empowered to lift the secrecy in question and acts accordingly.

~~*3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.*~~

~~*4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Article 18

Right to data portability

~~*1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.*~~

~~*2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.*~~

~~3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

Recitals

(51) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what *estimated* period, which recipients receive the data, what is the *general* logic of the data that are undergoing the processing and what might be, ~~at least when based on profiling,~~ the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property, *such as in relation to and in particular* the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.

~~(55)~~(51a) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. *Data controllers should be encouraged to develop interoperable formats that enable data portability.* This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract. *Providers of information society services should not make the transfer of those data mandatory for the provision of their services.*

COMP Article 16
11.10.2013

Article 16
Right to rectification

The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by providing a supplementary statement.

Recitals

(54a) Data which are contested by the data subject and whose accuracy or inaccuracy cannot be determined should be blocked until the issue is cleared.

COMP Article 17

17.10.2013

Article 17

Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, *and to obtain from third parties the erasure of any links to, or copy or replication of that data, especially in relation to personal data which are made available by the data subject while he or she was a child*, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;

(d) the ~~processing of the~~ data *has been unlawfully processed does not comply with this Regulation for other reasons.*

1a. The application of paragraph 1 shall be dependent upon the ability of the data controller to verify that the person requesting the erasure is the data subject.

2. Where the controller referred to in paragraph 1 has made the personal data public *without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article 77, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.*

3. The controller *and, where applicable, the third party* shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

- (a) for exercising the right of freedom of expression in accordance with Article 80;
- (b) for reasons of public interest in the area of public health in accordance with Article 81;
- (c) for historical, statistical and scientific research purposes in accordance with Article 83;
- (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect ***the essence of*** the right to the protection of personal data and be proportionate to the legitimate aim pursued;
- (e) in the cases referred to in paragraph 4.

4. Instead of erasure, the controller shall restrict processing of personal data ***in such a way that it is not subject to the normal data access and processing operations and can not be changed anymore***, where:

- (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;
- (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;
- (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;

(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be restricted;

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with paragraphs ***2a of Article 18(2) 15;***

(da) the particular type of storage technology does not allow for erasure and has been installed before the entry into force of this Regulation.

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

~~7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.~~

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

8a. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

9. The Commission shall be empowered to adopt, *after requesting an opinion of the European Data Protection Board*, delegated acts in accordance with Article 86 for the purpose of further specifying:

(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;

(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;

(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

Recitals

(53) Any person should have the right to have personal data concerning them rectified and a 'right to *erasure and to be forgotten*' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. *This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.* However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them. *Also, the right to erasure should not apply when the retention of personal data is necessary for the performance of a contract with the data subject, or when there is a legal obligation to retain this data.*

(54) To strengthen the 'right to *erasure 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 *without legal justification* should be obliged to *take all necessary steps to have the data erased, including by third parties, without prejudice to the right of the data subject to claim compensation. ~~inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.~~*

COMP Article 19

14.10.2013

Article 19

Right to object

1. The data subject shall have the right to object, ~~on grounds relating to their particular situation,~~ at any time to the processing of personal data which is based on points (d) ~~and~~ (e) ~~and (f)~~ of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where ~~the processing of~~ personal data ~~is are processed for direct marketing purposes is based on points (d), (e) and (f) of Article 6(1),~~ the data subject shall have *at any time and without any further justification*, the right to object free of charge *in general or for any particular purpose* to the processing of their personal data ~~for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.~~

2a. The ~~This~~ right *referred to in paragraph 2* shall be explicitly offered to the data subject in an intelligible manner *and form, using clear and plain language, in particular if addressed specifically to a child*, and shall be clearly distinguishable from other information.

2b. *In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the right to object may be exercised by automated means using a technical standard which allows the data subject to clearly express his or her wishes.*

3. Where an objection is upheld pursuant to paragraphs 1 and-2, the controller shall no longer use or otherwise process the personal data concerned *for the purposes determined in the objection.*

Recitals

(56) In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them, *free of charge and in a manner that can be easily and effectively invoked*. The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.

(57) Where ~~personal data are processed for the purposes of direct marketing,~~ the data subject ~~should have~~ has the right to object to ~~such the~~ processing, ~~free of charge and in a manner that can be easily and effectively invoked~~ *the controller should explicitly*

offer it to the data subject in an intelligible manner and form, using clear and plain language and should clearly distinguish it from other information.

COMP Article 20

16.10.2013

Article 20

Measures based on Profiling

1. ~~Without prejudice to the provisions in Article 6 every natural person shall have the right not to be subject to object to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. profiling in accordance with Article 19. The data subject shall be informed about the right to object to profiling in a highly visible manner.~~

2. Subject to the other provisions of this Regulation, a person may be subjected to ~~a measure of the kind referred to in paragraph 1~~ profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject only if the processing:

(a) is ~~carried out in the course of necessary for~~ the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied, *provided that or where* suitable measures to safeguard the data subject's legitimate interests have been adduced, ~~such as the right to obtain human intervention; or~~

(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests;

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. *Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling. Profiling shall not be based solely on the special categories of personal data referred to in Article 9.*

~~4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.~~

5. *Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment. The ~~Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for~~ suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 shall include the right to obtain human assessment and an explanation of the decision reached after such assessment.*

5a. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b) for further specifying the criteria and conditions for profiling pursuant to paragraph 2.

Recitals

*(58) Without prejudice to the lawfulness of the data processing, every natural person should have the right ~~not to be subject to object to a measures which is based on~~ profiling ~~by means of automated processing. However, such measures~~ Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject should **only** be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. The In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human **assessment intervention** and that such measure should not concern a child. **Such measures should not lead to discrimination against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity.***

(58a) Profiling based solely on the processing of pseudonymous data should be presumed not to significantly affect the interests, rights or freedoms of the data subject. Where profiling, whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute pseudonymous data to a specific data subject, the processed data should no longer be considered to be pseudonymous.

COMP Article 21

16.10.2013

Article 21 Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights ~~provided for~~ in ~~points (a) to (e) of Article 5 and~~ Articles 11 to ~~19 20~~ and Article 32, when such a restriction ~~constitutes~~ *meets a clearly defined objective of public interest, respects the essence of the right to protection of personal data, is proportionate to the legitimate aim pursued and respects the fundamental rights and interests of the data subject and is* a necessary and proportionate measure in a democratic society to safeguard:

- (a) public security;
- (b) the prevention, investigation, detection and prosecution of criminal offences;
- (c) ~~other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and~~ taxation matters ~~and the protection of market stability and integrity~~;
- (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- (e) a monitoring, inspection or regulatory function *in the framework of* ~~connected, even occasionally, with~~ the exercise of a *competent public official* authority in cases referred to in (a), (b), (c) and (d);
- (f) the protection of the data subject or the rights and freedoms of others.

2. In particular, any legislative measure referred to in paragraph 1 *must be necessary and proportionate in a democratic society and* shall contain specific provisions at least as to:

- (a) the objectives to be pursued by the processing ~~and~~;
- (b) the determination of the controller;
- (c) *the specific purposes and means of processing*;
- (d) *the safeguards to prevent abuse or unlawful access or transfer*;
- (e) *the right of data subjects to be informed about the restriction.*

2a. Legislative measures referred to in paragraph 1 shall neither permit nor oblige private controllers to retain data additional to those strictly necessary for the original purpose.

Recitals

(59) Restrictions on specific principles and on the rights of information, ~~access~~, rectification and erasure or on the right of **access and to obtain** data, the right to object, profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other **specific and well-defined** public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

COMP Article 22

15.10.2013

Article 22

Responsibility and accountability of the controller

1. The controller shall adopt *appropriate* policies and implement appropriate *and demonstrable technical and organizational* measures to ensure and be able to demonstrate *in a transparent manner* that the processing of personal data is performed in compliance with this Regulation, *having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself.*

1a. Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and updated where necessary.

~~2. The measures provided for in paragraph 1 shall in particular include:~~

~~(a) keeping the documentation pursuant to Article 28;~~

~~(b) implementing the data security requirements laid down in Article 30;~~

~~(c) performing a data protection impact assessment pursuant to Article 33;~~

~~(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);~~

~~(e) designating a data protection officer pursuant to Article 35(1);~~

3. The controller shall ~~implement mechanisms to ensure the verification of~~ be able to demonstrate the *adequacy and* effectiveness of the measures referred to in paragraphs 1 and 2. ~~If proportionate, this verification shall be carried out by independent internal or external auditors.~~ Any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, shall contain a summary description of the policies and measures referred to in paragraph 1.

3a. The controller shall have the right to transmit personal data inside the Union within the group of undertakings the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as

the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct as referred to in Article 38.

~~*4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized enterprises.*~~

Recitals

(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established, *in particular with regard to documentation, data security, impact assessments, the data protection officer and oversight by data protection authorities*. In particular, the controller should ensure and be *obliged able* to demonstrate the compliance of each processing operation with this Regulation. *This should be verified by independent internal or external auditors.*

COMP Article 23

16.10.2013

Article 23

Data protection by design and by default

1. Having regard to the state of the art, *current technical knowledge, and the cost of implementation, international best practices and the risks represented by the data processing*, the controller *and the processor, if any*, shall, both at the time of the determination of the *purposes and* means for processing and at the time of the processing itself, implement appropriate *and proportionate* technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, *in particular with regard to the principles laid out in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures.*

1a. In order to foster its widespread implementation in different economic sectors, data protection by design shall be a prerequisite for public procurement tenders according to the Directive of the European Parliament and of the Council on public procurement as well as according to the Directive of the European Parliament and of the Council on procurement by entities operating in the water, energy, transport and postal services sector (Utilities Directive).

2. The controller shall *ensure implement mechanisms for ensuring* that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, ~~or~~ retained *or disseminated* beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals *and that data subjects are able to control the distribution of their personal data.*

~~3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.~~

~~4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted, after requesting an~~

~~*opinion by the European Data Protection Board, in accordance with the examination procedure referred to in Article 87(2).*~~

Recitals

(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. ***The principle of data protection by design require data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation.***

COMP Article 24 14.10.2013

Article 24 Joint controllers

Where ~~a several~~ controllers ~~jointly~~ determines the purposes, ~~conditions~~ and means of the processing of personal data ~~jointly with others~~, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. *The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. In case of unclarity of the responsibility, the controllers shall be jointly and severally liable.*

Recitals

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller. *The arrangement between the joint controllers should reflect the joint controllers' effective roles and relationships. The processing of personal data under this Regulation should include the permission for a controller to transmit the data to a joint controller or to a processor for the processing of the data on their behalf.*

COMP Article 25

16.10.2013

Article 25

Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

2. This obligation shall not apply to:

(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

(b) ~~an enterprise employing fewer than 250 persons a controller processing personal data which relates to less than 5000 data subjects during any consecutive 12-month period and not processing special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems;~~ or

(c) a public authority or body; or

(d) a controller ~~offering~~ only occasionally *offering* goods or services to data subjects *residing* in the Union, *unless the processing of personal data concerns special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems.*

3. The representative shall be established in one of those Member States where ~~the data subjects whose personal data are processed in relation to~~ the offering of goods or services to *the data subjects them*, or *to the monitoring of them, take place reside.*

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Recitals

(63) Where a controller not established in the Union is processing personal data of data subjects *residing* in the Union ~~whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of their behaviour~~, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the ~~controller~~ *processing relates to fewer than 5000 data subjects during any consecutive 12-month period and is not carried out on special categories of personal data, or is* a public authority or body or where the controller is only occasionally offering goods or services to such data subjects.

The representative should act on behalf of the controller and may be addressed by any supervisory authority.

(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects *residing* in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities.

COMP Article 26

16.10.2013

Article 26

Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller. ~~and stipulating in particular that~~ The controller and the processor shall be free to determine respective roles and tasks with respect to the requirements of this Regulation, and shall provide that the processor shall:

(a) ~~not~~ process personal data only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited unless otherwise required by Union law or Member State law;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) determine the conditions for enlisting another processor only with the prior permission of the controller, unless otherwise determined.

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the ~~necessary~~ appropriate and relevant technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34, taking into account the nature of processing and the information available to the processor;

(g) return ~~hand-over~~ all results to the controller after the end of the processing, and not process the personal data otherwise and delete existing copies unless Union or Member State law requires storage of the data;

(h) make available to the controller ~~and the supervisory authority~~ all information necessary to ~~demonstrate control~~ compliance with the obligations laid down in this Article and allow on-site inspections;

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

3a. The sufficient guarantees referred to in paragraph 1 may be demonstrated by adherence to codes of conduct or certification mechanisms pursuant to Articles 38 or 39 of this Regulation.

4. If a processor processes personal data other than as instructed by the controller or becomes the determining party in relation to the purposes and means of data processing, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

COMP Article 27

14.10.2013

Article 27

Processing under the authority of the controller and processor

The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.

COMP Article 28
17.10.2013

Article 28
Documentation

1. Each controller and processor ~~and, if any, the controller's representative,~~ shall maintain **regularly updated** documentation necessary to fulfill the requirements laid down in this Regulation.

2. In addition, each controller and processor shall maintain documentation of the following information:

(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;

(b) the name and contact details of the data protection officer, if any;

(c) the name and contact details of the controllers to whom personal data are disclosed, if any.

Recitals

(65) In order to **be able to** demonstrate compliance with this Regulation, the controller or processor should maintain **the documentation document each processing operations necessary in order to fulfill the requirements laid down in this Regulation.** Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for ~~monitoring those processing operations~~ **evaluating the compliance with this Regulation. However, equal emphasis and significance should be placed on good practice and compliance and not just the completion of documentation.**

COMP Article 29
10.7.2013

Article 29
Co-operation with the supervisory authority

1. The controller and, *if any*, the processor and, ~~*if any*~~, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.