Version 14.10.2013

Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data
(COM(2012)0010 – C7-0024/2012 – 2012/0010(COD))

COMP Article 1

Article 1
Subject matter and objectives

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, ***the*** investigation, detection or prosecution of criminal offences **and** the execution of criminal penalties ***and conditions for the free movement of such personal data.***

2. In accordance with this Directive, Member States shall:

2(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of ***their*** personal data ***and privacy***; and

2(b) ensure that the exchange of personal data by competent authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

2a) This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive.

Recitals

(1) The protection of natural persons in relation to the processing of personal data is fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty of the Functioning of the European Union lay down that everyone has the right to the protection of personal data concerning him or her. ***Article 8(2) of the Charter of Fundamental Rights of the European Union lays down that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.***

(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.

(3)Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows competent authorities to make use of personal data on an unprecedented scale in order to pursue their activities.

(4) This requires facilitating the free flow of data, ***when necessary and proportionate***, between competent authorities within the Union and the transfer to third countries and international

organisations, while ensuring a high level of protection of personal data. These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement.

(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties must be equivalent in all Member States. ***Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.***

(8) Article 16(2) of the Treaty on the Functioning of the European Union provides that the European Parliament and the Council should 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 ***their*** personal data ***and privacy***.

(9) On that basis, Regulation EU …../2012 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) lays down general rules to protect of individuals in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

(10) In Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police co-operation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the Conference
acknowledged that specific rules on the protection of personal data and the free movement of such data in the fields of judicial co-operation in criminal matters and police co-operation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.

(11) Therefore a ***specific*** Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(14) The protection afforded by this Directive should concern natural persons, whatever their nationality or place of residence, in relation to the processing of personal data.

(70) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of ***their*** personal data and to ensure the free exchange of personal data by competent authorities within the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective***. Member States may provide for higher standards than those established in this Directive.***

(80) This Directive respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaty, notably the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on these rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Version 14.10.2013
COMP Article 2

Article 2

Scope

1. This Directive applies to the processing of personal data by competent authorities for the purposes referred to in Article 1(1).

2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

3. This Directive shall not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

Recitals

(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of judicial co-operation in criminal matters and police co-operation.

(6) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(12) In order to ensure the same level of protection for individuals through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, the Directive should provide harmonised rules for the protection and the free movement of personal data in the areas of judicial co-operation in criminal matters and police co-operation.

(13) This Directive allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Directive.

(15) The protection of individuals should be technological 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 Directive. This Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, in particular concerning national security, or to data processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust.

(76) In accordance with Articles 2 and 2a of the Protocol on the position of Denmark, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union,

Denmark is not bound by this Directive or subject to its application. ~~Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the Treaty on the Functioning of the European Union, Denmark shall, in accordance with Article 4 of that Protocol, decide within six months after adoption of this Directive whether it will implement it in its national law.~~

(77) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis.

(78) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis.

(79) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis.

Version 14.10.2013
COMP Article 3

Article 3
Definitions

For the purposes of this Directive:

~~(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 identifiers 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, restriction, 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) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(5) '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;

(6) 'controller' means the competent public authority 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;

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

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

(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 data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;

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

(14) 'competent authorities' means any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(15) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 39.

Recitals

(16) The principles of protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify ***or single out*** the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. ***This Directive*** should not apply to ***anonymous data, meaning any data that can not be related, directly or indirectly, alone or in combination with associated data, to a natural person. Given the importance of the developments under way in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate location data relating to natural persons, which may be used for different purposes including surveillance or creating profiles, this Directive should be applicable to processing involving such personal data.***

(17) Personal data relating to health should include in particular all data pertaining to the health status of a data subject, information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on, for example; a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

Version 14.10.2013
COMP Article 4

Article 4
Principles relating to personal data processing

Member States shall provide that personal data must be:

(a) processed lawfully***, fairly and in a transparent and verifiable manner in relation to the data subject;***

(b) collected for specified, explicit and legitimate purposes and not further ***processed in a way incompatible with those purposes.***

(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;***

(d) accurate and 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;

(e) kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed;

(f) processed under the responsibility and liability of the controller, who shall ensure ***and be able to demonstrate*** compliance with the provisions adopted pursuant to this Directive;

(fa)new processed in a way that effectively allows the data subject to exercise his or her rights as described in Articles 10 to 17;

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

(fc)new processed by only those duly authorised staff in competent authorities who need them for the performance of their tasks.

Recitals

(16a)new Any processing of personal data must be lawful, fair and transparent in relation towards 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 personal data. The personal data should be adequate, relevant and limited to the minimum necessary for the purposes for which the personal data are processed. This requires in particular limiting the data collected and the period for which the data are stored 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 should be rectified or deleted. In order to ensure that the data are kept no longer than necessary, time limits should be established by the controller for erasure or periodic review.

~~(18) Any processing of personal data must be fair and lawful in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit~~.

~~(19) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to retain and process personal data, collected in the context of the prevention,investigation, detection or prosecution of specific criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected.~~

~~(20) Personal data should not be processed for purposes incompatible with the purpose for which it was collected. Personal data should be adequate, relevant and not excessive for the purposes for which the personal data are processed. Every reasonable step should be taken to ensure that personal data which are inaccurate should be rectified or erased.~~

(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

~~(22) In the interpretation and application of the general principles relating to personal data processing by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, account should be taken of the specificities of the sector, including the specific objectives pursued~~**.**

Version 14.10.2013
COMP Article 4a

Article 4a (new)

1. Access to data initially processed for purposes other than those referred to in Article 1 (1)

Member States shall provide that competent authorities may only have access to personal data initially processed for purposes other than those referred to in Article 1(1) if they are specifically authorised by Union or Member State law which must meet the requirements set out in Article 7(1a) and must provide that:

(a) access is allowed only by duly authorised staff of the competent authorities in the performance of their tasks where, in a specific case, reasonable grounds give reason to believe that the processing of the personal data will substantially contribute to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(b) requests for access must be in writing and refer to the legal ground for the request; and

(c) the written request must documented; and

(d) appropriate safeguards are implemented to ensure the protection of fundamental rights and freedoms in relation to the processing of personal data. Those safeguards shall be without prejudice to and complementary to specific conditions of access to personal data such as judicial authorisation in accordance with Member State law.

2. Personal data held by private parties or other public authorities shall only be accessed to investigate or prosecute criminal offences in accordance with necessity and proportionality requirements to be defined by Union law by each Member State in its national law, in full compliance with article 7a).

(20a) The simple fact that two purposes both relate to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties does not necessarily mean that they are compatible. However, there are cases in which further processing for incompatible purposes should be possible if necessary to comply with a legal obligation to which the controller is subject, in order to protect the vital interests of the data subject or another person, or for the prevention of an immediate and serious threat to public security. Member States should therefore be able to adopt national laws providing for such derogations to the extent strictly necessary. Such national laws should contain adequate safeguards.

Version 14.10.2013

Article 4b (new)

Time limits of storage and review

1. Member States shall provide that personal data processed pursuant to this Directive shall be deleted by the competent authorities where they are no longer necessary for the purposes for which they were processed.

2. Member States shall provide that the competent authorities put mechanisms in place to ensure that time-limits, pursuant to Article 4, are established for the erasure of personal data and for a periodic review of the need for the storage of the data, including fixing storage periods for the different categories of personal data. Procedural measures shall be established to ensure that these time-limits or the periodic review intervals are observed.

Version 14.10.2013
COMP Article 5

Article 5

~~**Distinction between different categories of data subjects**~~

~~1. Member States shall provide that, as far as possible, the controller makes a clear distinction between personal data of different categories of data subjects, such as:~~

~~(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;~~

~~(b) persons convicted of a criminal offence;~~

~~(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;~~

~~(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b); and~~

~~(e) persons who do not fall within any of the categories referred to above.~~

Different categories of data subjects

1***. Member States shall provide that the competent authorities, for the purposes referred to in Article 1(1), may process personal data of the following different categories of data subjects, and the controller shall make a clear distinction between such categories:***

(a) persons with regard to whom there are reasonable grounds for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a crime;

(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;

(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b).

2. Personal data of other data subjects than those referred to under paragraph 1 may only be processed:

(a) as long as necessary for the investigation or prosecution of a specific criminal offence in order to assess the relevance of the data for one of the categories indicated in paragraph 1; or

(b) when such processing is indispensable for targeted, preventive purposes or for the purposes of criminal analysis, if and as long as this purpose is legitimate, well-defined and specific and the processing is strictly limited to assess the relevance of the date for one of the categories

indicated in paragraph 1. This is the subject to regular review at least every six months, any further use is prohibited.

3. Member States shall provide that additional limitations and safeguards, according to Member State law, apply to the further processing of personal data relating to data subjects referred to in paragraph 1(c) and (d).

Recitals

(23) It is inherent to the processing of personal data in the areas of judicial co-operation in criminal matters and police co-operation that personal data relating to different categories of data subjects are processed. Therefore a clear distinction should as far as possible be made between personal data of different categories of data subjects such as
suspects, persons convicted of a criminal offence, victims and third parties, such as witnesses, persons possessing relevant information or contacts and associates of suspects and convicted criminals. ***Specific rules on the consequences of this categorisation should be provided by the Member States, taking into account the different purposes for which data are collected and providing specific safeguards for persons who are not suspect or have not been convicted of a criminal offence.***

Version 14.10.2013
COMP Article 6

Article 6

Different degrees of accuracy and reliability of personal data

1. Member States shall ***provide*** that ***accuracy and reliability of personal data undergoing processing is ensured.***

2. Member States shall ensure that personal data based on facts are distinguished from personal data based on personal assessments***, in accordance with their degree of accuracy and reliability.***

2a Member States shall ensure that ***personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available***. ***To this end, the competent authorities shall assess the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, up-to-dateness and reliability. Personal data shall not be transmitted without request from a competent authority, in particular data originally held by private parties.***

2b ***If it emerges that incorrect data have been transmitted or data have been transmitted unlawfully, the recipient must be notified without delay. The recipient shall be obliged to rectify the data without delay in accordance with paragraph 1 and Article 15 or to erase them in accordance with Article 16.***

Recitals

(24) As far as possible personal data should be distinguished according to the degree of their accuracy and reliability. Facts should be distinguished from personal assessments, in order to ensure both the protection of individuals and the quality and reliability of the information processed by the competent authorities.

Version 14.10.2013
COMP Article 7

Article 7

Lawfulness of processing

1. Member States shall provide that the processing of personal data is lawful only if and to the extent that processing based on ***Union or Member State*** law for the purposes set out in Article 1(1) ***and it is necessary:***

(a) for the performance of a task carried out by a competent authority; or

(b) in order to protect the vital interests of the data subject or of another person; or

(c) for the prevention of an immediate and serious threat to public security.

1a.(new) Member State law regulating the processing of personal data within the scope of this Directive shall contain explicit and detailed provisions specifying at least:

(a) the objectives of the processing;

(b) the personal data to be processed;

(c) the specific purposes and means of processing;

(d) the appointment of the controller, or of the specific criteria for the appointment of the controller;

(e) the categories of duly authorised staff of the competent authorities for the processing of personal data;

(f) the procedure to be followed for the processing;

(g) the use that may be made of the personal data obtained;

(h) limitations on the scope of any discretion conferred on the competent authorities in relation to the processing activities.

Recitals

(25) In order to be lawful, the processing of personal data should be ***only allowed when*** necessary for compliance with a legal obligation to which the controller is subject, for the performance of a task carried out in the public interest by a competent authority based on ***Union or national*** law ***which should contain explicit and detailed provisions at least as to the objectives, the personal data, the specific purposes and means, designate or allow to designate the controller, the procedures to be followed, the use and limitations of the scope of any discretion conferred to the competent authorities in relation to the processing activities.***

Version 14.10.2013
COMP Article 7a

Article 7a

Further processing for incompatible purposes

1. Member States shall provide that personal data may only be further processed for another purpose set out in Article 1(1) which is not compatible with the purposes for which the data were initially collected if and to the extent that:

(a) the purpose is strictly necessary and proportionate in a democratic society and required by Union or Member State law for a legitimate, well-defined and specific purpose;

(b) the processing is strictly limited to a period not exceeding the time needed for the specific data processing operation;

(c) any further use for other purposes is prohibited;

Prior to any processing, the Member State shall consult the data protection supervisor and conduct a data protection impact assessment.

2. In addition to the requirements set out in Article 7(1a), Member State law authorising further processing as referred to in paragraph 1 shall contain explicit and detailed provisions specifying at least as to:

(a) the specific purposes and means of that particular processing;

(b) that access is allowed only by the duly authorised staff of the competent authorities in the performance of their tasks where in a specific case there are reasonable grounds for believing that the processing of the personal data will contribute substantially to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and

(c) that appropriate safeguards are established to ensure the protection of fundamental rights and freedoms in relation to the processing of personal data.

Member States may require that access to the personal data is subject to additional conditions such as judicial authorisation, in accordance with their national law.

3. Member States may also allow further processing of personal data for historical, statistical or scientific purposes provided that they establish appropriate safeguards, such as making the data anonymous.

Recitals

(25a) Personal data should not be processed for purposes incompatible with the purpose for which it was collected. Further processing by competent authorities for a purpose falling within the scope of this Directive which is not compatible with the initial purpose should only be authorised in specific cases where such processing is necessary for compliance with a legal obligation, based on Union or national law, to which the controller is subject, or in order to protect the vital interest of the data subject or of another person or for the prevention of an immediate and serious threat to public security. The fact that data are processed for a law

enforcement purpose does not necessarily imply that this purpose is compatible with the initial purpose. The concept of compatible use is to be interpreted restrictively.

(25b) Personal data processed in breach of the national provisions adopted pursuant to this Directive should not be longer processed.

Version 14.10.2013
COMP Article 8

Article 8

Processing of special categories of personal data

1. Member States shall prohibit 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 biometric*** data or data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the processing is ***strictly necessary and proportionate for the performance of a task carried out ~~in the public interest~~ by the competent authorities for the purposes set out in Article 1(1), on the basis of Union or Member State law which shall provide for specific and suitable measures to safeguard the data subject's legitimate interests, including specific authorisation from a judicial authority, if required by national law; or***

(b) the processing is necessary to protect the vital interests of the data subject or of another person; or

(c) the processing relates to data which are manifestly made public by the data subject***, provided that they are relevant and strictly necessary for the purpose pursued in a specific case.***

Recitals

(26) 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 processing is specifically ***necessary for the performance of a task carried out in the public interest, on the basis of Union or national*** law which provides for suitable measures to safeguard the data subject's ***fundamental rights and*** legitimate interests; or processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject. ***Sensitive personal data should be processed only if they supplement other personal data already processed for law enforcement purposes. Any derogation to the prohibition of processing of sensitive data should be interpreted restrictively and not lead to frequent, massive or structural processing of sensitive personal data.***

Version 14.10.2013
COMP Article 8a

Article 8a

Processing of genetic data for the purpose of a criminal investigation or a judicial procedure

1. Member States shall ensure that genetic data may only be used to establish a genetic link within the framework of adducing evidence, preventing a threat to public security or preventing the commission of a specific criminal offence. Genetic data may not be used to determine other characteristics which may be linked genetically.

2. Member States shall provide that genetic data or information derived from their analysis may only be retained as long as necessary for the purposes for which data are processed and where the individual concerned has been convicted of serious offences against the life, integrity or security of persons, subject to strict storage periods to be determined by Member State law.

3. Member States shall ensure that genetic data or information derived from their analysis is only stored for longer periods when the genetic data cannot be attributed to an individual, in particular when it is found at the scene of a crime.

Recitals

(26a) The processing of genetic data should only be allowed if there is a genetic link which appears in the course of a criminal investigation or a judicial procedure. Genetic data should only be stored as long as strictly necessary for the purpose of such investigations and procedures, while Member States can provide for longer storage under the conditions set out in this Directive.

Version 14.10.2013
COMP Article 9

Article 9
Measures based on profiling and automated processing

1. Member States shall provide that measures which produce ***a*** legal effect for the data subject or significantly affect them and which are ***partially or fully*** based on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.

2. Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based on special categories of personal data referred to in Article 8.

2a(new). Automated processing of personal data intended to single out a data subject without an initial suspicion that the data subject might have committed or will be committing a criminal offence shall only be lawful if and to the extent that it is strictly necessary for the investigation of a serious criminal offence or the prevention of a clear and imminent danger, established on factual indications, to public security, the existence of the state, or the life of persons.

2b(new). Profiling that (whether intentionally or otherwise) has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, gender or sexual orientation, or that (whether intentionally or otherwise) results in measures which have such effect, shall be prohibited in all cases.

Recitals

(27) Every natural person should have the right not to be subject to a measure which is based on ***on partially or fully profiling by means of*** automated processing***. Such processing which*** produces a legal effect for that person, ***or significantly affects them should be prohibited,*** unless authorised by law and subject to suitable measures to safeguard the data subject's ***fundamental rights and*** legitimate interests, ***including the right to be provided with meaningful information about the logic used in the profiling. Such processing should in no circumstances contain, generate, or discriminate based on special categories of data.***

Version 14.10.2013

CHAPTER III
RIGHTS OF THE DATA SUBJECT

COMP Article 9a (new)

Article 9a (new)
General principles for data subject rights

1. Member States shall ensure that 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 Directive aim to strengthen, clarify, guarantee and where appropriate, codify these rights.

2. Member States shall ensure that 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 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.

Version 14.10.2013
COMP Article 10

Article 10
Modalities for exercising the rights of the data subject

1. Member States shall provide that the controller ***has concise,*** transparent, ***clear*** and easily accessible policies with regard to the processing of personal data and for the exercise of the data subjects' rights.

2. Member States shall provide that any information and any communication relating to the processing of personal data are to be provided by the controller to the data subject in an intelligible form, using clear and plain language***, in particular where that information is addressed specifically to a child***.

3. Member States shall provide that the controller ***establishes*** procedures for providing the information referred to in Article 11 and for the exercise of the rights of data subjects referred to in Articles 12 to 17. ***Where personal data are processed by automated means, the controller shall provide means for requests to be made electronically.***

4. Member States shall provide that the controller informs the data subject about the follow-up given to their request without delay***, and in any event at the latest within one month of receipt of the request***. ***The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form.***

5. Member States shall provide that the information and any action taken by the controller following a request referred to in paragraphs 3 and 4 are 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 cost,*** for providing the information or taking the action requested. In that case, the controller shall bear the burden of proving the ***excessive*** character of the request.

5a(new) Member States may provide that the data subject may assert his or her rights directly against the controller or through the intermediary of the competent national supervisory authority. Where the supervisory authority has acted on the request of the data subject, the supervisory authority shall inform the data subject of the verifications carried out.

Recitals

(28) In order to exercise their rights, any information to the data subject should be easily accessible and easy to understand, including the use of clear and plain language. ***This information should be adapted to the needs of the data subject in particular when information is addressed specifically to a child.***

(29) Modalities should be provided for facilitating the data subject's exercise of their rights under this Directive, including mechanisms to request, free of charge, in particular access to data, rectification and erasure. The controller should be obliged to respond to requests of the data subject without delay ***and within one month of receipt of the request. Where personal data are processed by automated means the controller should provide means for requests to be made electronically.***

Version 14.10.2013
COMP Article 11

Article 11
Information to the data subject

1. Where personal data relating to a data subject are collected, Member States shall ensure that the controller ***provides*** the data subject with at least the following information:

(a) the identity and the contact details of the controller and of the data protection officer;

(b) ***the legal basis and*** the purposes of the processing for which the personal data are intended;

(c) the period for which the personal data will be stored;

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

(e) the right to lodge a complaint to the supervisory authority referred to in Article 39 and its contact details;

(f) the recipients of the personal data, including in third countries or international organisations ***~~and on potential access to the data, under the rules of that third country or international organisation~~; and who is authorised to access this data under the laws of that third country or the rules of that international organisation, the existence or absence of an adequacy decision by the Commission or in case of transfers referred to in Article 35 or Artcile 36, the means to obtain a copy of the appropriate safeguards used for the transfer;***

(fa) (new) where the controller processes personal data as described in Article 9(1), information about the existence of processing for a measure of the kind referred to in Article 9(1) and the intended effects of such processing on the data subject, information about the logic used in the profiling and the right to obtain human assessment;

(fb) (new) information regarding security measures taken to protect personal data;

(g) any further information in so far as such further information is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed.

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 or voluntary, as well as the possible consequences of failure to provide such data.

3. The controller shall provide the information referred to in paragraph 1:

(a) at the time when the personal data are obtained from the data subject, or

(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 processed.

4. Member States may adopt legislative measures delaying or restricting the provision of the information to the data subject***, in a specific case***, to the extent that, and as long as, such partial

or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the ***fundamental rights and the*** legitimate interests of the person concerned:

(a) to avoid obstructing official or legal inquiries, investigations or procedures ;

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;

(c) to protect public security;

(d) to protect national security;

(e) to protect the rights and freedoms of others.

5. ***Member States shall provide that the controller shall assess, in each specific case, by means of a concrete and individual examination, whether a partial or complete restriction for one of the reasons referred to in paragraph 4 applies.*** Member States may ***by law also*** determine categories of data processing which may wholly or partly fall under the exemptions ***under points (a), (b), (c) and (d)*** of paragraph 4.

Recitals

(30) The principle of fair ***and transparent*** processing requires that the data subjects should be informed in particular of the existence of the processing operation and its purposes, ***its legal basis,*** how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. ***Furthermore the data subject shall be informed if profiling takes place and its intended consequences***. 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.

(31) 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 obtained 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 processed.

Version 14.10.2013
COMP Article 12

Article 12
Right of access for the data subject

1. Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data relating to them are being processed. Where such personal data are being processed, the controller shall provide the following information***; if it has not already been provided:***

(aa) communication of the personal data undergoing processing and of any available information as to their source***, and if applicable, intelligible information about the logic involved in any automated processing***.

(ab) the significance and envisaged consequences of such processing, at least in the case of the measures referred to in Article 9.

(a) the purposes of the processing ***as well as the legal basis for the processing;***

(b) the categories of personal data concerned;

(c) the recipients to whom the personal data have been disclosed, in particular the recipients in third countries;

(d) the period for which the personal data will be stored;

(e) the existence of the right to request from the controller rectification, erasure or restriction of processing of personal data concerning the data subject;

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

2. Member States shall provide for the right of the data subject to obtain from the controller a copy of the personal data undergoing processing. ***Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.***

Recitals

(32) 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 of and verify the lawfulness of the processing. Every data subject should therefore have the right to know about and obtain communication in particular of the purposes for which the data are processed, ***the legal basis***, for what period, which recipients receive the data, including in third countries***, the intelligible information about the logic involved in any automated processing and its significant and envisaged consequences if applicable, and the right to lodge a complaint to the supervisory authority and its contact details.*** Data subjects should be allowed to receive a copy of their personal data which are being processed.

Version 14.10.2013
COMP Article 13

Article 13
Limitations to the right of access

1. Member States may adopt legislative measures restricting, wholly or partly, ***depending on the specific case,*** the data subject's right of access to the extent ***and for the period*** that such partial or complete restriction constitutes a ***strictly*** necessary and proportionate measure in a democratic society with due regard for the ***fundamental rights and the*** legitimate interests of the person concerned:

(a) to avoid obstructing official or legal inquiries, investigations or procedures;

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties;

(c) to protect public security;

(d) to protect national security;

(e) to protect the rights and freedoms of others.

2. Member States shall provide that the controller assesses, in each specific case by means of a concrete and individual examination whether a partial or complete restriction for one of the reasons referred to in paragraph 1 applies. Member States may also determine by law categories of data processing which may wholly or partly fall under the exemptions under points (a) to (d) of paragraph 1.

3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject, ***without undue delay,*** in writing on any refusal or restriction of access, on the reason***ed justification*** for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. The information on factual or legal reasons on which the decision is based may be omitted where the provision of such information would undermine a purpose under paragraph 1.

4. Member States shall ensure that the controller documents the ***assessment referred to in paragraph 2 as well as*** the grounds for ***restricting*** the communication of the factual or legal reasons on which the decision is based. ***That information shall be made available to the national supervisory authorities.***

Recitals

(33) Member States should be allowed to adopt legislative measures delaying ***or*** restricting the information of data subjects or the access to their personal data to the extent that and as long as such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the ***fundamental rights and the*** legitimate interests of the person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties, to protect public security or national security, or, to protect the data subject or the rights and freedoms of others. ***The controller should assess by way of concrete and individual examination of each case if partial or complete restriction of the right of access should apply.***

(34) Any refusal or restriction of access should be set out in writing to the data subject including the factual or legal reasons on which the decision is based.

(34a) Any restriction of the data subject's rights must be in compliance with the Charter of Fundamental Rights of the European Union and with the European Convention for the Protection of Human Rights and Freedoms, as clarified by the case law of the Court of Justice of the European Union and the European Court of Human Rights, and in particular respect the essence of the rights and freedoms.

Version 14.10.2013
COMP Article 14

Article 14
Modalities for exercising the right of access

1. Member States shall provide for the right of the data subject to request, ***at all times,*** in particular in cases referred to in Article ***12 and*** 13, that the supervisory authority checks the lawfulness of the processing.

2. Member ***States*** shall provide that the controller informs the data subject of the right to request the intervention of the supervisory authority pursuant to paragraph 1.

3. When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question. ***The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.***

3a. (new) Member States may provide that the data subject may assert this right directly against the controller or through the intermediary of the competent national supervisory authority.

3b. (new) Member States shall ensure that there are reasonable time limits for the controller to respond to requests of the data subject regarding their exercise of their right of access.

Recitals

(35) Where Member States have adopted legislative measures restricting wholly or partly the right to access, the data subject should have the right to request that the competent national supervisory authority checks the lawfulness of the processing. The data subject should be informed of this right. When access is exercised by the supervisory authority on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications by the supervisory authority have taken place and of the result as regards to the lawfulness of the processing in question. ***The supervisory authority should also inform the data subject of the right to seek a judicial remedy.***

Version 14.10.2013
COMP Article 15

Article 15
Right to rectification *and completion*

1. Member States shall provide for the right of the data subject to obtain from the controller the rectification ***or the completion*** of personal data relating to them which are inaccurate ***or incomplete***, in particular by way of a ***completing or*** corrective statement.

2. Member States shall provide that the controller informs the data subject in writing***, with a reasoned justification of*** any refusal ***of*** rectification ***or completion***, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

2a. (new) Member States shall provide that the controller shall communicate any rectification carried out to each recipient to whom the data have been disclosed, unless to do so proves impossible or involves a disproportionate effort.

2b. (new) Member States shall provide that the controller communicates the rectification of inaccurate personal data to the third party from which the inaccurate personal data originates.

2c. (new) Member States shall provide that the data subject may assert this right also through the intermediary of the competent national supervisory authority.

Recitals

(36) Any person should have the right to have inaccurate ***or unlawfully processed*** personal data concerning them rectified and the right of erasure where the processing of such data is not in compliance with the ***provisions*** laid down in this Directive. ***Such rectification, completion or erasure should be communicated to recipients to whom the data has been disclosed and to the third parties from which the inaccurate data originated. The controllers should also abstain from further dissemination of such data.*** Where the personal data are processed in the course of a criminal investigation and proceedings, rectification, the rights of information, access, erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.

Version 14.10.2013
COMP Article 16

Article 16
Right to erasure

1. Member States shall provide for the right of the data subject to obtain from the controller the erasure of personal data relating to them where the processing does not comply with the provisions adopted pursuant to ***Articles 4, 6,*** 7 and 8 of this Directive.

2. The controller shall carry out the erasure without delay. ***The controller shall also abstain from further dissemination of such data.***

3. Instead of erasure, the controller shall ***restrict the processing of*** the personal data 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 personal data have to be maintained for purposes of proof ***or for the protection of vital interests of the data subject or another person.***

3b. (new) Where processing of personal data is restricted pursuant to paragraph 3, the controller shall inform the data subject before lifting the restriction on processing

4. Member States shall provide that the controller informs the data subject in writing ***with a reasoned justification,*** of any refusal of erasure or ***restriction*** of the processing, ***on*** reasons for the refusal and ***on*** the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

4a. (new) Member States shall provide that the controller notifies recipients to whom these data have been sent of any erasure or restriction made pursuant to paragraph 1, unless to do so proves impossible or involves a disproportionate effort. The controller shall inform the data subject about those third parties.

4b. (new) Member States may provide that the data subject may assert this right directly against the controller or through the intermediary of the competent national supervisory authority.

Version 14.10.2013
COMP Article 17

Article 17
Rights of the data subject in criminal investigations and proceedings

Member States may provide that the rights of information, access, rectification, erasure and restriction of processing referred to in Articles 11 to 16 are carried out in accordance with national rules on judicial proceedings where the personal data are contained in a judicial decision or record processed in the course of criminal investigations and proceedings.

Recitals

(82) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access, rectification, erasure and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure.

Version 14.10.2013

CHAPTER IV
CONTROLLER AND PROCESSOR

SECTION 1
GENERAL OBLIGATIONS

COMP Article 18

Article 18
Responsibility of the controller

1. Member States shall provide that the controller adopts policies and implements appropriate measures to ensure ***and be able to demonstrate, in a transparent manner, for each processing operation,*** that the processing of personal data is performed in compliance with the provisions adopted pursuant to this Directive, ***both at the time of the determination of the means for processing and at the time of the processing itself.***

2. The measures referred to in paragraph 1 shall in particular include:

(a) keeping the documentation referred to in Article 23;

(aa) performing a data protection impact assessment pursuant to Article 25a;

(b) complying with the requirements for prior consultation pursuant to Article 26;

(c) implementing the data security requirements laid down in Article 27;

(d) designating a data protection officer pursuant to Article 30.

(da) drawing up and implementing specific safeguards in respect of the treatment of personal data relating to children, where appropriate.

3. The controller shall implement mechanisms to ensure the verification of the ***adequacy and*** effectiveness of the measures referred to in paragraph 1 of this Article. If proportionate, this verification shall be carried out by independent internal or external auditors.

Recitals

(37)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, the controller should ensure ***and be obliged to be able to demonstrate*** compliance of ***each*** processing operation with the rules adopted pursuant to this Directive.

Version 14.10.2013
COMP Article 19

Article 19
Data protection by design and by default

1. Member States shall provide that, 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 provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject, ***in particular with regard to the principles laid out in Article 4. 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 25a, the results shall be taken into account when developing those measures and procedures***.

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***.

Recitals

(38) The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of the Directive are met. In order to ensure compliance with the provisions adopted pursuant to this Directive, the controller should adopt policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.

Version 14.10.2013
COMP Article 20

Article 20
Joint controllers

1. Member States shall provide that where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers must determine the respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of ***a legally binding agreement*** between them.

2. Unless the data subject has been informed which of the joint controllers is responsible pursuant to paragraph 1, the data subject may exercise his or her rights under this Directive in respect of and against each of any two or more joint controllers.

Recitals

(39) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors requires a clear attribution of the responsibilities under this Directive, 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 data subject should have the right to exercise his or her rights under this Directive in respect of and against each of the joint controllers.(25) (covers 221)***

Version 14.10.2013
COMP Article 21

Article 21
Processor

1. Member States shall provide that where a processing operation is 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 the provisions adopted pursuant to this Directive 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 to ensure compliance with those measures.***

2. Member States shall provide that the carrying out of processing by ***means of*** a processor must be governed by a ***contract or*** legal act binding the processor to the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the ***controller;***

(b) employ only staff who have agreed to be bound by an obligation of confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 28;

(d) engage another processor only with the permission of the controller ***and therefore inform the controller of the intention to engage another processor in such a timely fashion that the controller has the possibility to object;***

(e) insofar as it is possible given the nature of the processing, adopt in agreement with controller the necessary 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 28 to 32;

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

(h) make available to the controller and the supervisory authority all the information necessary to verify compliance with the obligations laid down in this Article;

(i) take into account the principle of data protection by design and default.

2a. (new) The controller and the processor shall document in writing the controller's instructions and the processor's obligation referred to in paragraph 2.

3. If a processor processes personal data other than as instructed by the controller, 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 20.

Version 14.10.2013
COMP Article 22

Article 22
Processing under the authority of the controller and processor

Member States shall provide that the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, may only process them on instructions from the controller or where required by Union or Member State law.

1a. (new) Where the processor is or becomes the determining party in relation to the purposes, means, or methods of data processing or does not act exclusively on the instructions of the controller, it shall be considered a joint controller pursuant to Article 20.

Version 14.10.2013
COMP Article 23

Article 23
Documentation

1. Member States shall provide that each controller and processor maintains documentation of all processing systems and procedures under their responsibility.

2. The documentation shall contain at least the following information:

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

(aa) a legally binding agreement, where there are joint controllers; a list of processors and activities carried out by processors;

(b) the purposes of the processing;

(ba) an indication of the parts of the controller's or processor's organisation entrusted with the processing of personal data for a particular purpose;

(bb) a description of the category or categories of data subjects and of the data or categories of data relating to them;

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

(ca) where applicable, information about the existence of profiling, of measures based on profiling, and of mechanisms to object to profiling;

(cb) intelligible information about the logic involved in any automated processing;

(d) transfers of data to a third country or an international organisation, including the identification of that third country or international organisation ***and the legal grounds on which the data are transferred; a substantive explanation shall be given when a transfer is based on Articles 35 or 36 of this Directive;***

(da) the time limits for erasure of the different categories of data;

(db) the results of the verifications of the measures referred to in Article 20(1);

(dc) an indication of the legal basis of the processing operation for which the data are intended.

3. The controller and the processor shall make ***all*** documentation available, on request, to the supervisory authority.

Recitals

(40) Processing activities should be documented by the controller or processor, in order to monitor compliance with this Directive. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation available upon request, so that it might serve for monitoring processing operations.

(40a) Every processing operation of personal data should be recorded in order to enable the verification of the lawfulness of the data processing, selfmonitoring and ensuring proper data integrity and security. This record should be made available upon request to the supervisory authority for the purpose of monitoring compliance with the rules laid down in this Directive.

Version 14.10.2013
COMP Article 24

Article 24
Keeping of records

1. Member States shall ensure that records are kept of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The records of consultation and disclosure shall show in particular the purpose, date and time of such operations and as far as possible the identification of the person who consulted or disclosed personal data***, and the identity of the recipients of such data***.

2. The records shall be used solely for the purposes of verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security***, or for purposes of auditing, either by the data protection officer or by the data protection authority***.

2a. (new) The controller and the processor shall make the records available, on request, to the supervisory authority.

Version 14.10.2013
COMP Article 25

Article 25
Cooperation with the supervisory authority

1. Member States shall provide that the controller and the processor shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing ***the*** information ***referred to in Article 46(2)(a) and by granting access as provided in Article 46(2)(b).***

2. In response to the supervisory authority's exercise of its powers under points (a) and (b) of Article 46, 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.

Version 14.10.2013

COMP Article 25a (new)

Article 25a (new)
Data Protection impact assessment

1. Member States shall provide that~~, prior to the processing of personal data~~, the controller or the processor, acting on the controller´ s behalf, shall carry out an assessment of the impact of the envisaged processing systems and procedures on the protection of personal data, where the processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, prior to new processing operations or the earliest as possible in case of existing processing operations.

2. In particular the following processing operations are likely to present such specific risks as referred to in paragraph 1:

(a) processing of personal data in large scale filing systems for the purposes of the prevention, detection, investigation or prosecution of criminal offences and the execution of criminal penalties;

(b) processing of special categories of personal data as referred to in Article 8, of personal data related to children and of biometric and location data for the purposes of the prevention, detection, investigation or prosecution of criminal offences and the execution of criminal penalties.

(c) an evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's behaviour, which is based on automated processing and likely to result in measures that produces legal effects concerning the individual or significantly affects the individual;

(d) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance);

(e) other processing operations for which the consultation of the supervisory authority is required pursuant to Article 26(1).

3. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address those risks and minimise the volume of personal data which is processed;
(d) security measures and mechanisms to ensure the protection of personal data and to demonstrate the compliance with the provisions adopted pursuant to this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned;
(e) a general indication of the time limits for erasure of the different categories of data;
(f) where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in paragraph 2. of Article 36, the documentation of appropriate safeguards.

3a) If the controller or the processor has designated a data protection officer, he or she shall be involved in the impact assessment proceeding.

4. Member States shall provide that the controller consults the public on the intended processing, without prejudice to the protection of the public interests or the security of the processing operations.

5. Without prejudice to the protection of the public interests or the security of the processing operations, the assessment shall be made easily accessible to the public.

6. The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 56 for the purpose of specifying further the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability.

Recitals

(40b) A data protection impact assessment should be carried out by the controller or processor, where the processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, which should include in particular the envisaged measures, safeguards and mechanisms to ensure the protection of personal data and for demonstrating compliance with this Directive. Impact assessments should concern relevant systems and processes of personal data processing operations, but not individual cases.

Version 14.10.2013

COMP Article 26

Article 26

Prior consultation of the supervisory authority

1. Member States shall ensure that the controller or the processor consults the supervisory authority prior to the processing of personal data ***in order to ensure the compliance of the intended processing with the provisions adopted pursuant to this Directive and in particular to mitigate the risks involved for the data subjects where***:

(a) ***a data protection impact assessment as provided for in Article 25a indicates that processing operations by virtue of their nature, their scope and/or their purposes, are likely to present a high degree of specific risks; or***

(b) ***the supervisory authority deems it necessary to carry out a prior consultation on specified processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes***.

1a. (new) Where the supervisory authority determines in accordance with its power that the intended processing does not comply with the provisions adopted pursuant to this Directive, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.

2. Member States ***shall*** provide that the supervisory authority, ***after consulting the European Data Protection Board, shall establish*** a list of the processing operations which are subject to prior consultation pursuant to ***point (b) of paragraph 1***.

2a. (new) Member States shall provide that the controller or processor shall provide the supervisory authority with the data protection impact assessment pursuant to Article 25a and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

2b. (new) If the supervisory authority is of the opinion that the intended processing does not comply with the provisions adopted pursuant to this Directive or that the risks are insufficiently identified or mitigated, it shall make appropriate proposals to remedy such non-compliance.

2c. (new) Member States may consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing under this Directive, and in particular to mitigate the risks involved for the data subjects.

Recitals

(41) In order to ensure effective protection of the rights and freedoms of data subjects by way of preventive actions, the controller or processor should consult with the supervisory authority in certain cases prior to the processing. ***Moreover, where a data protection impact assessment indicates that processing operations are likely to present a high degree of specific risks to the rights and freedoms of data subjects, the supervisory authority should be in a position to prevent, prior to the start of operations, a risky processing which is not in compliance with this Directive, and to make proposals to remedy such situation. Such consultation may equally take place in the course of the preparation either of a measure of the national parliament or of a***

measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.

Version 14.10.2013
COMP Article 27

SECTION 2
DATA SECURITY

Article 27
Security of processing

1. Member States shall provide that the controller and the processor implements appropriate technical and organisational measures ***and procedures*** to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

2. In respect of automated data processing, each Member State shall provide that the controller or processor, following an evaluation of the risks, implements measures designed to:

(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

(b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(i) ensure that installed systems may, in case of interruption, be restored (recovery);

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity).

(ja) ensure that in case of sensitive personal data processing according to Article 8, additional security measures have to be in place, in order to guarantee situation awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data.

2a. (new) Member States shall provide that processors may be appointed only if they guarantee that they observe the requisite technical and organisational measures under paragraph 1 and comply with the instructions under Article 21(2)(a). The competent authority shall monitor the processor in those respects.

3. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, notably encryption standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

Recitals

41a (new)

In order to maintain security and to prevent processing in breach of this Directive, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, technological neutrality should be promoted.

Version 14.10.2013
COMP Article 28

Article 28
Notification of a personal data breach to the supervisory authority

1. Member States shall provide that in the case of a personal data breach, the controller notifies, without undue delay and, where feasible, not later than 24 hours ~~after having become aware of it,~~ the personal data breach to the supervisory authority. The controller shall provide, on request, to the supervisory authority a reasoned justification in cases ***of any delay.*** ~~where the notification is not made within 24 hours~~.

2. The processor shall alert and inform the controller ***without undue delay*** ~~immediately~~ after ***the establishment of a personal data breach.*** ~~having become aware of a personal data breach.~~

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) communicate the identity and contact details of the data protection officer referred to in Article 30 or other contact point where more information can be obtained;

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;

(d) describe the possible consequences of the personal data breach;

(e) describe the measures proposed or taken by the controller to address the personal data breach ***and mitigate its effects.***

In case all information cannot be provided without undue delay, the controller can complete the notification in a second phase.

4. Member States shall provide that the controller documents any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must ***be sufficient to*** enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

4a. (new) The supervisory authority shall keep a public register of the types of breaches notified.

5. The Commission shall be empowered to adopt***, after requesting an opinion of the European Data Protection Board,*** delegated acts in accordance with Article 56 for the purpose of specifying further the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission~~, after requesting an opinion of the European Data Protection Board~~***,*** may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2).

(42) A personal data breach may, if not addressed in an adequate and timely manner, result in ***a substantial economic loss and social*** harm, including ***identity fraud,*** to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, it should notify the breach to the competent national authority. The individuals whose personal data or privacy could be adversely affected by the breach should be notified without delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of an individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the processing of personal data. ***The notification should include information about measures taken by the provider to address the breach, as well as recommendations for the subscriber or individual concerned. Notifications to data subject should be made as soon as feasible and in close cooperation with the supervisory authority and respecting guidance provided by it.***

(43) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of misuse. Moreover, such rules and procedures should take into account the legitimate interests of competent authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

Version 14.10.2013
COMP Article 29

Article 29
Communication of a personal data breach to the data subject

1. Member States shall provide that when the personal data breach is likely to adversely affect the protection of the personal data, ~~or~~ ***the*** privacy, ***the rights or the legitimate interests*** of the data subject, the controller shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall ***be comprehensive and use clear and plain language***. ***It shall*** describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) ~~and~~ (c), ***and (d)*** of Article 28(3) ***and information about the rights of the data subject, including redress*.**

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the personal data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

3a. (new) Without prejudice to the controller's obligation to notify the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

4. The communication to the data subject may be delayed, ***or*** restricted ~~or omitted~~ on the grounds referred to in Article 11(4).

SECTION 3
DATA PROTECTION OFFICER

Article 30
Designation of the data protection officer

1. Member States shall provide that the controller or the processor designates a data protection officer.

2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32. ***The necessary level of expert knowledge shall be determined in particular according by the data processing carried out and the protection required for the personal data processed by the controller or the processor.***

2a. (new) Member States shall provide that the controller or the processor ensures that any other professional duties of the data protection officer are compatible with that person's tasks and duties as data protection officer and do not result in a conflict of interests.

2b (new). The data protection officer shall be appointed for a period of at least four years. The data protection officer may be reappointed for further terms. During the term of office, the data protection officer may only be dismissed from that function, if they no longer fulfil the conditions required for the performance of their duties.

2c. (new) Member States shall provide for the data subject the right to contact the data protection officer on all issues related to the processing of his or her personal data.

3a. Member States shall provide that the controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

Recitals

(44) The controller or the processor should designate a person who would assist the controller or processor to monitor ***and demonstrate*** compliance with the provisions adopted pursuant to this Directive. ***Where several competent authorities are acting under the supervision of a central authority, at least this central authority should designate such data protection officer.*** The data protection officers must be in a position to perform their duties and tasks independently and effectively, ***in particular by establishing rules that avoid conflict of interest with other tasks performed by the data protection officer.***

Version 14.10.2013
COMP Article 31

Article 31
Position of the data protection officer

1. Member States shall provide that the controller or the processor ensures that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. The controller or processor shall ensure that the data protection officer is provided with the means to perform duties and tasks referred to under Article 32 effectively and independently, and does not receive any instructions as regards the exercise of the function. ~~***The data protection officer shall directly report to the management of the controller or the processor.***~~

2a. The controller or the processor shall support the data protection officer in performing his or her tasks and shall provide all the means, including staff, premises, equipment, continuous professional training and any other resources necessary to carry out the duties and tasks referred to in Article 32, and to maintain his or her professional knowledge.

Version 14.10.2013
COMP Article 32

Article 32
Tasks of the data protection officer

Member States shall provide that the controller or the processor entrusts the data protection officer at least with the following tasks:

(a) ***to raise awareness,*** to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive, ***in particular with regards to technical and organisational measures and procedures*** and to document this activity and the responses received;

(b) to monitor the implementation and application of the policies in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations and the related audits;

(c) to monitor the implementation and application of the provisions adopted pursuant to this Directive, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under the provisions adopted pursuant to this Directive;

(d) to ensure that the documentation referred to in Article 23 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 28 and 29;

(f) to monitor ***the application of the data protection impact assessment by the controller or processor and*** the application for prior ~~authorisation~~ consultation to the supervisory authority, if required pursuant to ***Article 26(1)***

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on his own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on the data protection officer's own initiative.

Version 14.10.2013
COMP Article 33

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 33
General principles for transfers of personal data

Member States shall provide that any transfer of personal data by competent authorities that is undergoing processing or is intended for processing after transfer to a third country, or to an international organisation, including further onward transfer to another third country or international organisation, may take place only if:

(a) the ***specific*** transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(aa) the data are transferred to a controller in a third country or international organisation that is an public authority competent for the purposes referred in Article 1(1);**(**

(ab) the conditions laid down in this Chaprter ~~Articles 34 to 37~~ are complied with by the controller and the processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation;

(b) the ***other provisions adopted pursuant to this Directive*** are complied with by the controller and processor***; and***

(ba) the level of protection of the personal data individuals guaranteed in the Union by this Directive is not undermined.

(bb) ~~where~~ the Commission has decided under the conditions and procedure referred to in Article 34 that the third country or international organisation in question ensures an adequate level of protection; or

(bc) ~~where~~ appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument as referred to in Article 35.

~~2. Member States shall provide that a transfer, subject to the conditions set out in paragraph 1, may only take place:~~

~~(a) where the Commission has decided under the conditions and procedure referred to in Article 34 that the third country or international organisation in question ensures an adequate level of protection; or~~

~~(b) where appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument as referred to in Article 35.~~

Member States shall provide that further onward transfers referred to in paragraph 1 of this Article may only take place if, in addition to the conditions laid out in that paragraph:
(a) the onward transfer is necessary for the same specific purpose as the original transfer; and
(b) the competent authority that carried out the original transfer authorises the onward transfer.

Version 14.10.2013

Recitals

(45) Member States should ensure that a transfer to a third country only takes place if ***this specific transfer*** is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the controller in the third country or international organisation is ***a public authority*** competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced, ***or where appropriate safeguards have been adduced by way of a legally binding instrument***. ***Data transferred to competent public authorities in third countries should not be further processed for purposes other than the one they were transferred for.***

(45a) Further onward transfers from competent authorities in third countries or international organisations to which personal data have been transferred should only be allowed if the onward transfer is necessary for the same specific purpose as the original transfer and the second recipient is also a competent public authority. Further onward transfers should not be allowed for general law-enforcement purposes. The competent authority that carried out the original transfer should have agreed to the onward transfer.

Version 14.10.2013
COMP Article 34

Article 34
Transfers with an adequacy decision

1. Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided ~~***in accordance with Article 41 of Regulation (EU) …./2012 or***~~ in accordance with paragraph 3 of this Article that the third country or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any ~~further~~ ***specific*** authorisation.

2. ***When assessing the adequacy of the level of protection*** ~~Where no decision adopted in accordance~~ ~~***Article 41 of Regulation (EU) …./2012 exists***~~, the Commission shall ~~***assess the adequacy of the level of protection, giving***~~ ***give*** consideration to the following elements:

(a) the rule of law, relevant legislation in force, including concerning public security, defence, national security and criminal law as well as the ***implementation of this legislation and the*** security measures which are complied with in that country or by that international organisation; ***jurisprudential precedents*** as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules***, including sufficient sanctioning powers***, for assisting and advising the data subject in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation in question has entered into, ***in particular any legally binding conventions or instruments with respect to the protection of personal data***.

3. The Commission ***shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 56 to*** decide, within the scope of this Directive, that a third country or a territory or a processing sector within that third country or an international organisation ensures an adequate level of protection within the meaning of paragraph 2.

4. The ***delegated*** act shall specify its geographical and sectoral application, and identify the supervisory authority mentioned in point (b) of paragraph 2.

4a. The Commission shall, on an on-going basis, monitor developments that could affect the fulfilment of the elements listed in paragraph 2 in third countries and international organisations in relation to which a delegated act pursuant to paragraph 3 has been adopted.

5. The Commission shall be empowered to adopt, ~~after requesting an opinion of the European Data Protection Board,~~ delegated acts in accordance with Article 56 to decide within the scope of this Directive that a third country or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2, in particular in cases where the relevant legislation in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects whose personal data are being transferred.

6. Member States shall ensure that where the Commission decides pursuant to paragraph 5, that any transfer of personal data to the third country ~~or a territory or a processing sector within that third country,~~ or the international organisation in question shall be prohibited. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.

7. The Commission shall publish in the Official Journal of the European Union a list of those third countries, territories and processing sectors within a third country or an international organisation where it has decided that an adequate level of protection is or is not ensured.

8. The Commission shall monitor the application of the ***~~implementing~~ delegated*** acts referred to in paragraphs 3 and 5.

Recitals

(46) The Commission may decide with effect for the entire Union that certain third countries, or a territory within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.

(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how the rule of law, access to justice, as well as international human rights norms and standards, in that third country are respected.

(48) The Commission should equally be able to recognise that a third country, or a territory or a processing sector within a third country, or an international organisation, does not offer an adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited except when they are based on an international agreement, appropriate safeguards or a derogation. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. However, such a Commission decision shall be without prejudice to the possibility to undertake transfers on the basis of appropriate safeguards ***by means of legally binding instruments*** or on the basis of a derogation laid down in this Directive.

Version 14.10.2013
COMP Article 35

Article 35
Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, ***or decides that a third country, or a territory within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5),*** a controller or processor may ***not*** transfer personal data to a third country, territory or an international organisation ~~***only if***~~ ***unless*** the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

2. These transfers must be ***authorised by the supervisory authority prior to the transfer.*** ~~documented and the documentation must be made available to the supervisory authority on request~~.

Recitals

(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data.

Version 14.10.2013
COMP Article 36

Article 36
Derogations

1. Where the Commission concludes pursuant to Article 34(5) that an adequate level of protection does not exist, personal data may not be transferred to the third ~~country or a territory or a processing sector within that third country,~~ or the international organisation in question, if, in the case in question, the legitimate interests of the data subject in preventing any such transfer outweigh the public interest in transferring such data.

2. By way of derogation from Articles 34 and 35, Member States shall provide that a transfer of personal data to a third country or an international organisation may take place only on condition that:

(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or

(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or

(c) the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or

(d) the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or

(e) the transfer is necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty.

2a. Processing based on paragraph 2 must have a legal basis in Union law, or the law of the Member State to which the controller is subject; that law must meet public interest objective or the need to protect the rights and freedoms of others, respects the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

2b. All transfers of data decided on the basis of derogations shall be duly justified and shall be limited to what is strictly necessary, and frequent massive transfers of data shall not be allowed.

2c. The decision for transfers under paragraph 1 must be made by duly authorised staff. These transfers must be documented and the documentation must be made available to the supervisory authority on request, including the date and time of the transfer, information about the recipient authority, the justification for the transfer and the data transferred.

Recitals

(49a) In cases where no grounds for allowing a transfer exist, derogations should be allowed if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of

criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims. These derogations should be interpreted restrictively and should not allow frequent, massive and structural transfer of personal data and should not allow wholesale transfer of data which should be limited to data strictly necessary. Moreover, the decision for transfer should be made by a duly authorised person and this transfer must be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.

Version 14.10.2013
COMP Article 37

Article 37
Specific conditions for the transfer of personal data

Member States shall provide that the controller informs the recipient of the personal data of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met. ***The controller shall also notify the recipient of the personal data of any update, rectification or erasure of data, and the recipient shall in turn make the corresponding notification in the event that the data has subsequently been transferred.***

Version 14.10.2013
COMP Article 38

Article 38
International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:

(a) develop effective international co-operation mechanisms to ensure ~~facilitate~~ the enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice.

(da) clarify and ~~resolve~~ consult on jurisdictional conflicts with third countries.

2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or with international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 34(3).

Recitals

(50) When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights to protect themselves from the unlawful use or disclosure of that data. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information with their foreign counterparts.

Version 14.10.2013
COMP Article 38a

Article 38a
Report by the Commission

The Commission shall submit a report on the application of Articles 33 to 38 to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Directive. For that purpose, the Commission may request information from the Member States and supervisory authorities, which shall supply this information without undue delay. The report shall be made public.

Version 14.10.2013

CHAPTER VI
INDEPENDENT SUPERVISORY AUTHORITIES
SECTION I
INDEPENDENT STATUS

COMP Article 39

Article 39
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of the provisions adopted pursuant to this Directive and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For this purpose, the supervisory authorities shall co-operate with each other and the Commission.

2. Member States may provide that the supervisory authority established in Member States pursuant to Regulation (EU)…./2012 assumes responsibility for the tasks of the supervisory authority to be established pursuant to paragraph 1 of this Article.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board.

Recitals

(51) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions pursuant to this Directive and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data. For that purpose, the supervisory authorities should co-operate with each other. **(35)**

(52) Member States may entrust a supervisory authority already established in Member States under Regulation (EU)…./2012 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(53) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with adequate financial and human resources, premises and infrastructure, ***including technical capabilities, experience and skills,*** which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and cooperation with other supervisory authorities throughout the Union;

Version 14.10.2013
COMP Article 40

Article 40
Independence

1. Member States shall ensure that the supervisory authority acts with complete independence in exercising the duties and powers entrusted to it, ***notwithstanding co- operation and consistency arrangements pursuant to Chapter VII of this Directive.***

2. Each Member State shall provide that the members of the supervisory authority, in the performance of their duties, neither seek nor take instructions from anybody, ***and maintain complete independence and impartiality.***

3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.

5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers including those to be carried out in the context of mutual assistance, co-operation and active participation in the European Data Protection Board.

6. Each Member State shall ensure that the supervisory authority must have its own staff which shall be appointed by and subject to the direction of the head of the supervisory authority.

7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.

Version 14.10.2013
COMP Article 41

Article 41
General conditions for the members of the supervisory authority

1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.

2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties are demonstrated.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.

4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.

5. Where the term of office expires or the member resigns, the member shall continue to exercise their duties until a new member is appointed.

Recitals

(54) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government, ***on the basis of the consultation of the parliament,*** of the Member State, and include rules on the personal qualification of the members and the position of those members.

COMP Article 42

Article 42
Rules on the establishment of the supervisory authority

Each Member State shall provide by law:

(a) the establishment and status of the supervisory authority in accordance with Articles 39 and 40;

(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;

(c) the rules and procedures for the appointment of the members of the supervisory authority, as well as the rules on actions or occupations incompatible with the duties of the office;

(d) the duration of the term of the members of the supervisory authority, which shall be no less than four years, except for the first appointment after entry into force of this Directive, part of which may take place for a shorter period;

(e) whether the members of the supervisory authority shall be eligible for reappointment;

(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;

(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including where they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.

Version 14.10.2013
COMP Article 43

Article 43
Professional secrecy

Member States shall provide that the members and the staff of the supervisory authority are subject, both during and after their term of office ***and in conformity with national legislation and practice,*** to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties, ***whilst conducting their duties with independence and transparency as set out in this Directive.***

Version 14.10.2013
SECTION 2
DUTIES AND POWERS

COMP Article 44

Article 44
Competence

1. Member States shall provide that each supervisory authority ***is competent to perform the duties and to*** exercises, on the territory of its own Member State, the powers conferred on it in accordance with this Directive.

2. Member States shall provide that the supervisory authority is not competent to supervise processing operations of courts when acting in their judicial capacity.

Recitals

(55) While this Directive applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when they are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law.

Version 14.10.2013
COMP Article 45

Article 45
Duties

1. Member States shall provide that the supervisory authority:

(a) monitors and ensures the application of the provisions adopted pursuant to this Directive and its implementing measures;

(b) hears complaints lodged by any data subject, or by an association in accordance with Article 50, investigates, to the extent appropriate, the matter and informs the data subject the association of the progress and the outcome of the complaint within a reasonable period, in particular where further investigation or coordination with another supervisory authority is necessary;

(c) checks the lawfulness of data processing pursuant to Article 14, and informs the data subject within a reasonable period on the outcome of the check or on the reasons why the check has not been carried out;

(d) provides mutual assistance to other supervisory authorities and ensures the consistency of application and enforcement of the provisions adopted pursuant to this Directive;

(e) conducts investigations***, inspections and audits***, either on its own initiative or on the basis of a complaint, or on request of another supervisory authority, and informs the data subject concerned, if the data subject has addressed a complaint, of the outcome of the investigations within a reasonable period;

(f) monitors relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(g) is consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

(h) is consulted on processing operations pursuant to Article 26;

(i) participates in the activities of the European Data Protection Board

2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.

3. The supervisory authority shall, upon request, advise any data subject in exercising the rights laid down in provisions adopted pursuant to this Directive, and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.

5. Member States shall provide that the performance of the duties of the supervisory authority shall be free of charge for the data subject.

6. Where requests are vexatious, in particular due to their repetitive character, the supervisory authority may charge a ***reasonable*** fee. ***Such a fee shall not exceed the costs of taking the action requested.*** The supervisory authority shall bear the burden of proving of the vexatious character of the request.

Recitals

(56) In order to ensure consistent monitoring and enforcement of this Directive throughout the Union, the supervisory authorities should have the same duties and effective powers in each Member State, including ***effective*** powers of investigation, ***power to access all personal data and all information necessary for the performance of each supervisory function, power to access any of the premises of the data controller or the processor including data processing requirements, and*** legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings.

(57) Each supervisory authority should hear complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.

Version 14.10.2013
COMP Article 46

Article 46
Powers

1. Member States shall provide that each supervisory authority ***has the power***:

(a) ***to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;***

(b) ***to order the controller to comply with the data subject's requests to exercise his or her rights under this Directive, including those provided by Articles 12 to 17 where such requests have been refused in breach of those provisions;***

(c) ***to order the controller or the processor to provide information pursuant to Article 10(1) and (2) and Articles 11, 28 and 29;***

(d) to ensure compliance with opinions on prior consultations referred to in Article 26;

(e) to warn or admonish the controller or the processor;

(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions adopted pursuant to this Directive and the notification of such actions to third parties to whom the data have been disclosed;

(g) to impose a temporary or definitive ban on processing;

(h) to suspend data flows to a recipient in a third country or to an international organisation;

(i) to inform national parliaments, the government or other public institutions as well as the public on the matter.

2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:

(a) access to all personal data and to all information necessary for the performance of its supervisory duties,

(b) access to any of its premises, including to any data processing equipment and means, in accordance with national law, where there are reasonable grounds for presuming that an activity in violation of the provisions adopted pursuant to this Directive is being carried out there, without prejudice to a judicial authorisation if required by national law.

3. Without prejudice to Article 43, Member States shall provide that no additional secrecy requirements shall be issued to the requests of supervisory authorities.

4. Member States may provide that additional security screening in line with national law is required for access to information classified at a level similar to EU CONFIDENTIAL or higher. If no additional security screening is required under the law of the Member State of the relevant supervisory authority, this must be recognised by all other Member States.

5. Each supervisory authority shall have the power to bring violations of the provisions adopted pursuant to this Directive to the attention of the judicial authorities and to engage in legal proceedings and bring an action to the competent court pursuant to Article 53(2).

6. Each supervisory authority shall have the power to impose penalties in respect of administrative offences.

Version 14.10.2013
COMP AM Article 46a

Article 46a
Reporting of violations

1. Member States shall provide that the supervisory authorities take into account guidance issued by the European Data Protection Board pursuant to Article 66(4b) of Regulation (EU) ..../2012 and shall put in place effective mechanisms to encourage confidential reporting of breaches of this Directive.

2. Member States shall provide that the competent authorities shall put in place effective mechanisms to encourage confidential reporting of breaches of this Directive.

Version 14.10.2013
COMP Article 47

Article 47
Activities report

Member States shall provide that each supervisory authority draws up ~~an annual~~ ***a*** report on its activities, ***at least every two years***. The report shall be made available to the public, ***the respective Parliament,*** the Commission and the European Data Protection Board. ***It shall include information on the extent to which competent authorities in their jurisdiction have accessed data held by private parties to investigate or prosecute criminal offences***.

Version 14.10.2013
COMP Article 48

Article 48
Mutual assistance

1. Member States shall provide that supervisory authorities provide each other with mutual assistance in order to implement and apply the provisions pursuant to this Directive in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior consultations, inspections and investigations.

2. Member States shall provide that a supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority. ***Such measures may include, in particular, the transmission of relevant information or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Directive without delay and not later than one month after having received the request.***

2a. The request for assistance shall contain all the necessary information, including the purpose of the request, and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.

2b. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:
(a) it is not competent to deal with the request; or
(b) compliance with the request would be incompatible with the provisions adopted pursuant to this Directive.

3. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.

3a. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.

3b. No fee shall be charged for any action taken following a request for mutual assistance.

Recitals

(58) The supervisory authorities should assist one another in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive. ***Each supervisory authority should be ready to participate in joint operations. The requested supervisory authority should be obliged to respond in a defined time period to the request.***

Version 14.10.2013
COMP Article 48a

Article 48a
Joint operations

1. Member States shall provide that, in order to step up cooperation and mutual assistance, the supervisory authorities may carry out joint enforcement measures and other joint operations in which designated members or staff from supervisory authorities of other Member States participate in operations within a Member State's territory.

2. Member States shall provide that in cases where data subjects in another Member State or other Member States are likely to be affected by processing operations, the competent supervisory authority may be invited to participate in the joint operations. The competent supervisory authority may invite the supervisory authority of each of those Member States to take part in the respective operation and in case where it is invited, respond to the request of a supervisory authority to participate in the operations without delay.

3. Member States shall lay down the practical aspects of specific co-operation actions.

Version 14.10.2013
COMP Article 49

Article 49
Tasks of the European Data Protection Board

1. The European Data Protection Board established by Regulation (EU)…./2012 shall exercise the following tasks in relation to processing within the scope of this Directive:

(a) advise the ***Union institutions*** on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;

(b) examine, on request of the Commission***, the European Parliament or the Council*** or on its own initiative or of one of its members, any question covering the application of the provisions adopted pursuant to this Directive and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of those provisions***, including on the use of enforcement powers***;

(c) review the practical application of guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;

(d) give the Commission an opinion on the level of protection in third countries or international organisations;

(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities***, including the coordination of joint operations and other joint activities where it so decides at the request of one or more supervisory authorities***;

(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

(g) promote the exchange of knowledge and documentation with data protection supervisory authorities worldwide, including data protection legislation and practice.

(ga) give its opinion to the Commission in the preparation of delegated and implementing acts under this Directive.

2. Where ***the European Parliament, the Council or*** the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 57(1) and make them public.

4. The Commission shall inform the European Data Protection Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

Recitals

(59) The European Data Protection Board established by Regulation (EU)…./2012 should contribute to the consistent application of this Directive throughout the Union, including advising the ***Union institutions,*** promoting the co-operation of the supervisory authorities throughout the Union, ***and give its opinion to the Commission in the preparation of delegated and implementing acts based on this Directive.***

Version 14.10.2013
CHAPTER VIII
REMEDIES, LIABILITY AND SANCTIONS

COMP Article 50

Article 50
Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for the right of every data subject to lodge a complaint with a supervisory authority in any Member State, if they consider that the processing of personal data relating to them does not comply with provisions adopted pursuant to this Directive.

2. Member States shall provide for the right of any body, organisation or association ***acting in the public interest*** which ***has been*** properly constituted according to the law of a Member State to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects, if it considers that a data subject's rights under this Directive have been infringed as a result of the processing of personal data.

3. Member States shall provide for the right of any body, organisation or association referred to in paragraph 2, independently of a data subject's complaint, to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.

Recitals

(60) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Directive are infringed or where the supervisory authority does not act on a complaint or does not act where such action is necessary to protect the rights of the data subject.

(61) Any body, organisation or association ***acting in the public interest*** constituted according to the law of a Member State should have the right to lodge a complaint or exercise the right to a judicial remedy on behalf of data subjects if duly mandated by them, or to lodge, independently of a data subject's complaint, its own complaint where it considers that a personal data breach has occurred.

Version 14.10.2013
COMP Article 51

Article 51
Right to a judicial remedy against a supervisory authority

1. Member States shall provide for the right ***for each natural or legal person*** to a judicial remedy against decisions of a supervisory authority ***concerning them***.

2. ***Member States shall provide that each*** data subject shall have the right to a judicial remedy for obliging the supervisory authority to act on a complaint, in the absence of a decision which is necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 45(1).

3. Member States shall provide that proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

3a. Member States shall ensure that final decisions by the court referred to in this Article will be enforced.

Recitals

(62) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established.

Version 14.10.2013
COMP Article 52

Article 52
Right to a judicial remedy against a controller or processor

1.Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority, Member States shall provide for the right of every natural person to a judicial remedy if they consider that that their rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of their personal data in non-compliance with these provisions.

1a. Member States shall ensure that final decisions by the court referred to in this Article will be enforced.

Recitals

(63) Member States should ensure that court actions, in order to be effective, allow the rapid adoption of measures to remedy or prevent an infringement of this Directive.

Version 14.10.2013
COMP Article 53

Article 53
Common rules for court proceedings

1. Member States shall provide for the right of any body, organisation or association referred to in Article 50(2) to exercise the rights referred to in Articles 51, 52 ***and 54 when mandated by*** one or more data subjects.

2. ***Member States shall provide that each*** supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions adopted pursuant to this Directive or to ensure consistency of the protection of personal data within the Union.

3. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.

Article 54
Liability and the right to compensation

1. Member States shall provide that any person who has suffered damage***, including non pecuniary damage,*** as a result of an unlawful processing operation or of an action incompatible with the provisions adopted pursuant to this Directive shall have the right to ***claim*** compensation from the controller or the processor for the damage suffered.

2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.

3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or processor proves that they are not responsible for the event giving rise to the damage.

Recitals

(64) Any damage, ***including non pecuniary damage***, which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where they establish fault on the part of the data subject or in case of force majeure.

Article 55
Penalties

Member States shall lay down the rules on penalties, applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.

Recitals

(65) Penalties should be imposed on any natural or legal person, whether governed by private or public law, that fails to comply with this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and must take all measures to implement the penalties.

Version 14.10.2013

Chapter VIIIa
Transmission of personal data to other parties

COMP Article 55a(new)

Article 55a(new)
Transmission of personal data to other authorities or private parties in the Union

1. Member States shall ensure that the controller does not transmit or instruct the processor to transmit personal data to a natural or legal person not subject to the provisions adopted pursuant to this Directive, unless:
(a) the transmission complies with Union or national law; and
(b) the recipient is established in a Member State of the European Union; and
(c) no legitimate specific interests of the data subject prevent transmission; and
(d) the transmission is necessary in a specific case for the controller transmitting the personal data for:
(i) the performance of a task lawfully assigned to it; or
(ii) the prevention of an immediate and serious danger to public security; or
(iii) the prevention of serious harm to the rights of individuals.
2. The controller shall inform the recipient of the purpose for which the personal data may exclusively be processed.
3. The controller shall inform the supervisory authority of such transmissions.
4. The controller shall inform the recipient of processing restrictions and ensure that these restrictions are met.

Recitals

(65a) Transmission of personal data to other authorities or private parties in the Union is prohibited unless the transmission is in compliance with law, and the recipient is established in a Member State, and no legitimate specific interests of the data subject prevent transmission, and the transmission is necessary in a specific case for the controller transmitting the data for either the performance of a task lawfully assigned to it, or the prevention of an immediate and serious danger to public security, or the prevention of serious harm to the rights of individuals. The controller should inform the recipient of the purpose of the processing and the supervisory authority of the transmission. The recipient should also be informed of processing restrictions and ensure that they are met.

Version 14.10.2013
CHAPTER IX
DELEGATED ACTS AND IMPLEMENTING ACTS

COMP Article 56

Article 56
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in ***Article 25a(6),*** Article 28(5), ***Article 34(3) and Article 34(5)*** shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Directive.

3. The delegation of power referred to in ***Article 25a(6),*** Article 28(5), ***Article 34(3) and Article 34(5)*** may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to ***Article 25a(6),*** Article 28(5), ***Article 34(3) and Article 34(5)*** shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of ***six*** months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by ***six*** months at the initiative of the European Parliament or the Council.

Recitals

(66) In order to fulfil the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent authorities within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of notifications of a personal data breach to the supervisory authority ***and as regards the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation***. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level***, in particular with the European Data Protection Board.*** The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.

Version 14.10.2013
COMP Article 56a(new)

Article 56a(new)
Deadline for the adoption of delegated acts

1. The Commission shall adopt the delegated acts under Article 25a(6) and Article 28(5) by [six months before the date referred to in Article 62(1)]. The Commission may extend the deadline referred to in this paragraph by six months.

Version 14.10.2013
COMP Article 57

Article 57
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

~~***3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.***~~

Recitals

(67) In order to ensure uniform conditions for the implementation of this Directive as regards documentation by controllers and processors, security of processing, notably in relation to encryption standards, notification of a personal data breach to the supervisory authority, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers.

(68) The examination procedure should be used for the adoption of measures as regards security of processing and notification of a personal data breach to the supervisory authority, given that those acts are of general scope.

~~(69) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection, imperative grounds of urgency so require~~**.**

Version 14.10.2013
COMP Article 58

Article 58
Repeals

1. Council Framework Decision 2008/977/JHA is repealed.

2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.

Recitals

(71) Framework Decision 2008/977/JHA should be repealed by this Directive.

(75) In accordance with Article 6a of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland shall not be bound by the rules laid down in this Directive where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.

Version 14.10.2013
COMP Article 59

Article 59
Relation with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation

The specific provisions for the protection of personal data with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive remain unaffected.

Recitals

(72) Specific provisions with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected. ***Moreover, this Directive should not apply to the processing of personal data carried out by the Union institutions, bodies, offices and agencies, which are governed by different legal instruments. As a result, this Directive does not entirely remedy the existing lack of comprehensiveness of the data protection legal rules in the Union and the uneven level of protection of the rights of data subjects. Since Article 8 of the Charter of Fundamental Rights and Article 16 TFEU imply that the fundamental right to the protection of personal data should be ensured in a consistent and homogeneous manner through the Union,*** the Commission should, ***within two years after the entry into force of this Directive***, evaluate the situation with regard to the relation between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, ***and should present appropriate proposals with a view to ensuring consistent and homogeneous legal rules relating to the processing of personal data by competent authorities or the access of designated authorities of Member States to information systems established pursuant to the Treaties as well as the processing of personal data by Union institutions, bodies, offices and agencies for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties within the scope of this Directive.***

(74) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011.

Version 14.10.2013
COMP Article 60

Article 60
Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation

International agreements concluded by Member States prior to the entry force of this Directive shall be amended, where necessary, within five years after the entry into force of this Directive.

Recitals

(73) In order to ensure a comprehensive and coherent protection of personal data in the Union, international agreements concluded by ***the Union or by the*** Member States prior to the entry force of this Directive should be amended in line with this Directive.

Version 14.10.2013
COMP Article 61

Article 61
Evaluation

1. The Commission shall, ***after requesting an opinion of the European Data Protection Board,*** evaluate the application ***and implementation*** of this Directive. ***It shall coordinate in close cooperation with the Member States and shall include announced and unannounced visits. The European Parliament and the Council shall be kept informed throughout the process and shall have access to the relevant documents.***

2. The Commission shall review within ***two years*** after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, in particular those acts adopted by the Union referred to in Article 59, and shall make appropriate proposals ***with a view to ensuring consistent and homogeneous legal rules relating to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*** within the scope of this Directive.

2a. The Commission shall present within two years of the entry into force of this Directive appropriate proposal for the revision of the legal framework applicable to the processing of personal data by Union institutions, bodies, offices and agencies, for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties with a view to ensuring consistent and homogeneous legal rules relating to the fundamental right to the protection of personal data in the Union.

3. The Commission shall submit reports on the evaluation and review of this Directive pursuant to paragraph 1 to the European Parliament and the Council at regular intervals. The first reports shall be submitted no later than four years after the entry into force of this Directive. Subsequent reports shall be submitted every four years thereafter. The Commission shall submit, if necessary, appropriate proposals with a view of amending this Directive and aligning other legal instruments. The report shall be made public.

Version 14.10.2013
COMP Article 62

Article 62
Implementation

1. Member States shall adopt and publish, by [date/ two years after entry into force] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions.
They shall apply those provisions from xx.xx.201x [date/ two years after entry into force].
When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Recitals

(81) In accordance with the Joint Political Declaration of Member States and the Commission on explanatory documents of 28 September 2011, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

Article 63
Entry into force and application

This Directive shall enter into force on the first day following that of its publication in the *Official Journal of the European Union*.

Article 64
Addressees

This Directive is addressed to the Member States.

Done at Brussels, 25.1.2012

For the European Parliament

The President

For the Council
The President