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

Compromise amendments on Articles 30-91

COMP Article 30
17.10.2013

Article 30
Security of processing

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing ***~~and the nature of the personal data to be protected~~***, ***taking into account the results of a data protection impact assessment pursuant to Article 33,*** having regard to the state of the art and the costs of their implementation.

1a. Having regard to the state of the art and the cost of implementation, such a security policy shall include:
(a) the ability to ensure that the integrity of the personal data is validated;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;
(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services;
(d) in the case of sensitive personal data processing according to Articles 8 and 9, additional security measures to ensure situational 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;
(e) a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.

2. The ***~~controller and the processor~~*** ***measures referred to in paragraph 1*** shall***~~, following an evaluation of the risks, take the measures referred to in paragraph 1 to~~*** ***at least:***
(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;
(b) protect personal data ***stored or transmitted*** against accidental or unlawful destruction, ***~~or~~*** accidental loss ***or alteration, and unauthorised or unlawful storage, ~~and to prevent any unlawful forms of~~, ~~in particular any unauthorised~~*** processing, ***access or*** disclosure, ***~~dissemination, or access~~***; and
(c) ensure the implementation of a security policy with respect to the processing of personal data.

3. The ***European Data Protection Board ~~Commission~~*** shall be ***entrusted with the task ~~empowered to adopt delegated acts in accordance with Article 86 for the purpose~~*** of ***issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b) ~~further specifying the criteria and conditions~~*** for the technical and organizational

measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, ~~***unless paragraph 4 applies***~~.

~~***4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:***~~
~~***(a) prevent any unauthorised access to personal data;***~~
~~***(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;***~~
~~***(c) ensure the verification of the lawfulness of processing operations.***~~
~~***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).***~~

Recitals

(66) In order to maintain security and to prevent processing in breach of this Regulation, 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, ~~***the Commission should promote***~~ technological neutrality, interoperability and innovation ***should be promoted***, and, where appropriate, ***cooperation with*** third countries ***should be encouraged***.

COMP Article 31
17.10.2013

Article 31
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay ~~*and, where feasible, not later than 24 hours after having become aware of it,*~~ **notify the personal data breach to the supervisory authority.** ~~*The notification to the supervisory authority shall be accompanied by a reasoned justification where it is not made within 24 hours*~~**.**

2. ~~*Pursuant to point (f) of Article 26(2), T*~~**he processor shall alert and inform the controller** *without undue delay* ~~*immediately*~~ **after the establishment of a personal data breach.**

3. The notification referred to in paragraph 1 must 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 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 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***.**
The information may if necessary be provided in phases.

4. The controller shall document 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** *and with Article 30***. The documentation shall only include the information necessary for that purpose.**

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

5. The *European Data Protection Board* ~~*Commission*~~ **shall be** *entrusted with the task* ~~*empowered to adopt delegated acts in accordance with Article 86 for the purpose*~~ **of** *issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b)* ~~*further specifying the criteria and requirements*~~ **for establishing the data breach** *and determining the undue delay* **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 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 87(2).*~~

Recitals

(67) A personal data breach may, if not addressed in an adequate and timely manner, result in 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,*~~ **the controller should notify the breach to the supervisory authority without undue delay,** *which should be presumed to be not later than* ~~*and, where feasible, within*~~ *72* **hours.** ~~*Where this cannot be achieved within 24 hours*~~*. If applicable,* **an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue 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 a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.**

COMP Article 32
10.7.2013

Article 32
Communication of a personal data breach to the data subject

1. 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 31, 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 31(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 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.

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

5. The *European Data Protection Board* ~~*Commission*~~ **shall be** *entrusted with the task* ~~*empowered to adopt delegated acts in accordance with Article 86 for the purpose*~~ **of** *issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b)* ~~*further specifying the criteria and requirements*~~ **as to the circumstances in which a personal data breach is likely to adversely affect the personal data** *or the privacy, the rights or the legitimate interests of the data subject* **referred to in paragraph 1.**

~~*6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

COMP Article 32a (-33, first Article of Section 3 of Chapter IV)
17.10.2013

Article 32a
Respect to Risk

1. The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks.

2. The following processing operations are likely to present specific risks:

(a) processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;

(b) processing of special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large scale filing systems;

(c) profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;

(d) processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

(e) automated monitoring of publicly accessible areas on a large scale;

(f) other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2);

(g) where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject;

(h) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects;

(i) where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.

3. According to the result of the risk analysis:

(a) where any of the processing operations referred to in paragraph 2 (a) or (b) exist, controllers not established in the Union shall designate a representative in the Union in line with the requirements and exemptions laid down in Article 25;

(b) where any of the processing operations referred to in paragraph 2 (a), (b) or (h) exist, the controller shall designate a data protection officer in line with the requirements and exemptions laid down in Article 35;

(c) where any of the processing operations referred to in paragraph 2 (a), (b), (c), (d), (e), (f), (g) or (h) exist, the controller or the processor acting on the controller's behalf shall carry out a data protection impact assessment pursuant to Article 33;

(d) where processing operations referred to in paragraph 2 (f) exist, the controller shall consult the data protection officer, or in case a data protection officer has not been appointed, the supervisory authority pursuant to Article 34.

4. The risk analysis shall be reviewed at the latest after one year, or immediately, if the nature, the scope or the purposes of the data processing operations change significantly. Where pursuant to paragraph 3 (c) the controller is not obliged to carry out a data protection impact assessment, the risk analysis shall be documented.

COMP Article 33
16.10.2013

Chapter 4 – section 3 – title

LIFECYCLE DATA PROTECTION ***MANAGEMENT*** ~~***IMPACT ASSESSMENT AND PRIOR AUTHORISATION***~~

Article 33
Data protection impact assessment

1. ***Where required pursuant to point c of Article 32a(3)*** ~~***where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,***~~ the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the ***rights and freedoms of the data subjects, especially their right to*** protection of personal data. ***A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.***

~~***The following processing operations in particular present specific risks referred to in paragraph 1:***~~

~~***(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;***~~

~~***(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;***~~

~~***(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;***~~

~~***(d) personal data in large scale filing systems on children, genetic data or biometric data;***~~

~~***(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).***~~

3. The assessment shall ***have regard to the entire lifecycle management of personal data from collection to processing to deletion. It shall*** contain at least
(a) a ***systematic*** description of the envisaged processing operations, ***the purposes of the processing and, if applicable, the legitimate interests pursued by the controller,***

(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, ***including the risk of discrimination being embedded in or reinforced by the operation,***

(d) a description of the measures envisaged to address the risks ***and minimise the volume of personal data which is processed***,

(e) a list of safeguards, security measures and mechanisms to ensure the protection of personal data, ***such as pseudonymisation,*** and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned;

(f) a general indication of the time limits for erasure of the different categories of data;

(h) an explanation which data protection by design and default practices pursuant to Article 23 have been implemented;

(i) a list of the recipients or categories of recipients of the personal data;

(j) 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 point (h) of Article 44(1), the documentation of appropriate safeguards;

(k) an assessment of the context of the data processing.

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

3b. The assessment shall be documented and lay down a schedule for regular periodic data protection compliance reviews pursuant to Article 33a(1). The assessment shall be updated without undue delay, if the results of the data protection compliance review referred to in Article 33a show compliance inconsistencies. The controller and the processor and, if any, the controller's representative, shall make the assessment available, on request, to the supervisory authority.

~~***4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.***~~

~~***5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.***~~

~~***6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the 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. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.*~~

~~*7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Recitals

(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those 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. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

(71) This should in particular apply to newly established large scale filing systems, which aim at processing a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.

(71a) Impact assessments are the essential core of any sustainable data protection framework, making sure that businesses are aware from the outset of all possible consequences of their data processing operations. If impact assessments are thorough, the likelihood of any data breach or privacy-intrusive operation can be fundamentally limited. Data protection impact assessments should consequently have regard to the entire lifecycle management of personal data from collection to processing to deletion, describing in detail the envisaged processing operations, the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure compliance with the regulation.

~~*(73) Data protection impact assessments should be carried out by a public authority or public body if such an assessment has not already been made in the context of the adoption of the national law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question.*~~

COMP Article 33a
7.10.2013

Article 33a
Data protection compliance review

1. At the latest two years after the carrying out of an impact assessment pursuant to Article 33(1), the controller or the processor acting on the controller's behalf shall carry out a compliance review. This compliance review shall demonstrate that the processing of personal data is performed in compliance with the data protection impact assessment.

2. The compliance review shall be carried out periodically at least once every two years, or immediately when there is a change in the specific risks presented by the processing operations.

3. Where the compliance review results show compliance inconsistencies, the compliance review shall include recommendations on how to achieve full compliance.

4. The compliance review and its recommendations shall be documented. The controller and the processor and, if any, the controller's representative, shall make the compliance review available, on request, to the supervisory authority.

5. If the controller or the processor has designated a data protection officer, he or she shall be involved in the compliance review proceeding.

Recital

(71a) Controllers should focus on the protection of personal data throughout the entire data lifecycle from collection to processing to deletion by investing from the outset in a sustainable data management framework and by following it up with a comprehensive compliance mechanism.

COMP Article 34
7.10.2012

Article 34
***~~Prior authorisation and p~~*Prior consultation**

~~1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data personal data to a third country or an international organisation.~~

2. The controller or processor acting on the controller's behalf shall consult the ***data protection officer, or in case a data protection officer has not been appointed, the*** supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

(b) ***the data protection officer*** *or* the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3. Where the ***competent*** supervisory authority ***determines in accordance with its power~~ is of the opinion~~*** that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

4. The ***European Data Protection Board ~~supervisory authority~~*** shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to ***~~point (b) of~~*** paragraph 2. ***~~The supervisory authority shall communicate those lists to the European Data Protection Board.~~***

~~5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.~~

6. The controller or processor shall provide the supervisory authority, ***on request***, with the data protection impact assessment ***pursuant to ~~provided for in~~*** Article 33 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.

7. Member States shall 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 with this Regulation and in particular to mitigate the risks involved for the data subjects.

~~***8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.***~~

~~***9. The Commission may set out standard forms and procedures for prior authorizations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).***~~

Recitals

(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, ***the data protection officer or*** the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. ~~***Such***~~ ***A*** consultation ***of the supervisory authority*** should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.

(74a) Impact assessments can only be of help if controllers make sure that they comply with the promises originally laid down in them. Data controllers should therefore conduct periodic data protection compliance reviews demonstrating that the data processing mechanisms in place comply with assurances made in the data protection impact assessment. It should further demonstrate the ability of the data controller to comply with the autonomous choices of data subjects. In addition, in case the review finds compliance inconsistencies, it should highlight these and present recommendations on how to achieve full compliance.

COMP Article 35
17.10.2013

Article 35
Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body; or

(b) the processing is carried out by ***a legal person and relates to more than 5000 data subjects in any consecutive 12-month period*** ~~***an enterprise employing 250 persons or more,***~~ or

(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects***; or***.

(d) the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1), location data or data on children or employees in large scale filing systems.

2. ~~***In the case referred to in point (b) of paragraph 1,***~~ A group of undertakings may appoint a ***main responsible*** data protection officer, ***provided it is ensured that a data protection officer is easily accessible from each establishment***.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. The controller or processor shall designate the data protection officer 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 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

7. The controller or the processor shall designate a data protection officer for a period of at least ***four*** ~~***two***~~ years ***in case of an employee or two years in case of an external service contractor***. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed if the data protection officer no longer fulfils the conditions required for the performance of their duties.

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. 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.

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

~~11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of or the controller or the processor referred to in point (c) of paragraph 1 and the criteria for professional qualities of the data protection officer referred to in paragraph 5.~~

Recitals

(75) Where the processing is carried out in the public sector or where, in the private sector, processing ***relates to more than 5000 data subjects within 12 months ~~is carried out by a large enterprise~~,*** or where its core activities, regardless of the size of the enterprise, involve processing operations ***on sensitive data, or processing operations*** which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. ***When establishing whether data about a large number of data subjects are processed, archived data that is restricted in such a way that they are not subject to the normal data access and processing operations of the controller and can no longer be changed should not be taken into account.*** Such data protection officers, whether or not an employee of the controller ***and whether or not performing that task full time***, should be in a position to perform their duties and tasks independently ***and enjoy special protection against dismissal. Final responsibility should stay with the management of an organization. The data protection officer should in particular be consulted prior to the design, procurement, development and setting-up of systems for the automated processing of personal data, in order to ensure the principles of privacy by design and privacy by default.***

(75a) ***The data protection officer should have at least the following qualifications: extensive knowledge of the substance and application of data protection law, including technical and organizational measures and procedures; mastery of technical requirements for privacy by design, privacy by default and data security; industry-specific knowledge in accordance with the size of the controller or processor and the sensitivity of the data to be processed; the ability to carry out inspections, consultation, documentation, and log file analysis; and the ability to work with employee representation. The controller should enable the data protection officer to take part in advanced training measures to maintain the specialized knowledge required to perform his or her duties. The designation as a data protection officer does not necessarily require fulltime occupation of the respective employee.***

COMP Article 36
7.10.2013

Article 36
Position of the data protection officer

1. The controller or the processor shall ensure 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 performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the ***executive*** management of the controller or the processor. ***The controller or processor shall for this purpose designate an executive management member who shall be responsible for the compliance with the provisions of this Regulation.***

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide ***all means, including*** staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37***, and to maintain his or her professional knowledge***.

4. Data protection officers shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from that obligation by the data subject.

COMP Article 37
17.10.2013

Article 37
Tasks of the data protection officer

1. The controller or the processor shall entrust 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 pursuant to this Regulation***, in particular with regard 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 of the controller or processor 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 this Regulation, 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 this Regulation;

(d) to ensure that the documentation referred to in Article 28 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior ~~***authorisation or prior***~~ consultation, if required pursuant Articles ***32a,*** 33 and 34;

(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 the data protection officer's 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 his/her own initiative~~.~~***;***

(i) to verify the compliance with this Regulation under the prior consultation mechanism laid out in Article 34;

(j) to inform the employee representatives on data processing of the employees.

~~***2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks,***~~

~~*certification, status, powers and resources of the data protection officer referred to in paragraph 1.*~~

COMP Article 38
15.10.2013

Article 38
Codes of conduct

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct ***or the adoption of codes of conduct drawn up by a supervisory authority*** intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

(a) fair and transparent data processing;
(aa) respect for consumer rights;
(b) the collection of data;
(c) the information of the public and of data subjects;
(d) requests of data subjects in exercise of their rights;
(e) information and protection of children;
(f) transfer of data to third countries or international organisations;
(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;
(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority ***shall without undue delay*** ~~***may***~~ give an opinion in whether ***the processing under*** the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

3. Associations and other bodies representing categories of controllers ***or processors*** in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.

4. The Commission ***shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86*** ~~***may adopt implementing acts***~~ for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 ***are in line with this Regulation and*** have general validity within the Union. ***This delegated act shall confer enforceable rights on data subjects.*** ~~***Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).***~~

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Recitals

(76) Associations or other bodies representing categories of controllers should be encouraged, ***after consultation of the representatives of the employees,*** to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors. ***Such codes should make compliance with this Regulation easier for industry.***

COMP Article 39
14.10.2013

Article 39
Certification

1. ~~***The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.***~~

1a. Any controller or processor may request any supervisory authority in the Union, for a reasonable fee taking into account the administrative costs, to certify that the processing of personal data is performed in compliance with this Regulation, in particular with the principles set out in Article 5, 23 and 30, the obligations of the controller and the processor, and the data subject's rights.

1b. The certification shall be voluntary, affordable, and available via a process that is transparent and not unduly burdensome.

1c. The supervisory authorities and the European Data Protection Board shall cooperate under the consistency mechanism pursuant to Article 57 to guarantee a harmonised data protection certification mechanism including harmonised fees within the Union.

1d. During the certification procedure, the supervisory authority may accredit specialised third party auditors to carry out the auditing of the controller or the processor on their behalf. Third party auditors shall have sufficiently qualified staff, be impartial and free from any conflict of interests regarding their duties. Supervisory authorities shall revoke accreditation, if there are reasons to believe that the auditor does not fulfil its duties correctly. The final certification shall be provided by the supervisory authority.

1e. Supervisory authorities shall grant controllers and processors, who pursuant to the auditing have been certified that they process personal data in compliance with this Regulation, the standardised data protection mark named "European Data Protection Seal".

1f. The "European Data Protection Seal" shall be valid for as long as the data processing operations of the certified controller or processor continue to fully comply with this Regulation.

1g. Notwithstanding paragraph 1f, the certification shall be valid for maximum five years.

1h. The European Data Protection Board shall establish a public electronic register in which all valid and invalid certificates which have been issued in the Member States can be viewed by the public.

~~***2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.***~~

2a. The European Data Protection Board may on its own initiative certify that a data protection-enhancing technical standard is compliant with this Regulation.

3. The Commission shall be empowered to adopt***, after requesting an opinion of the European Data Protection Board and consulting with stakeholders, in particular industry and non-governmental organisations,*** delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1***-1h***, including ***requirements for accreditation of auditors,*** conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries. ***These delegated acts shall confer enforceable rights on data subjects.***

Recitals

(77) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and ***standardised*** marks should be encouraged, allowing data subjects to quickly***, reliably and verifiably*** assess the level of data protection of relevant products and services. ***A "European Data Protection Seal" should be established on the European level to create trust among data subjects, legal certainty for controllers, and at the same time export European data protection standards by allowing non-European companies to more easily enter European markets by being certified***.

COMP AM Article 40
14.10.2013

Article 40
General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and 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.

Recitals

(78) Cross-border flows of personal data are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, ***the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined. In any event, transfers to third countries may only be carried out in full compliance with this Regulation.***

(79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects ***ensuring an adequate level of protection for the fundamental rights of citizens***.

COMP AM Article 41
16.10.2013

Article 41
Transfers with an adequacy decision

1. A transfer may take place where the Commission has decided 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 ***specific*** ~~***further***~~ authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law ***as well as the implementation of this legislation***, the professional rules and 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 subjects 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 delegated acts in accordance with Article 86 to*** ~~***may***~~ decide 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. ~~***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).***~~ ***Such delegated acts shall provide for a sunset clause if they concern a processing sector and shall be revoked according to paragraph 5 as soon as an adequate level of protection according to this Regulation is no longer ensured.***

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

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

5. The Commission ***shall be empowered to adopt delegated acts in accordance with Article 86 to*** ~~***may***~~ decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure ***or no longer ensures*** an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, 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 residing in the Union whose personal data are being transferred. ~~***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).***~~

6. Where the Commission decides pursuant to paragraph 5, 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, without prejudice to Articles 42 to 44. 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.

6a. Prior to adopting a delegated act pursuant to paragraphs 3 and 5, the Commission shall request the European Data Protection Board to provide an opinion on the adequacy of the level of protection. To that end, the Commission shall provide the European Data Protection Board with all necessary documentation, including correspondence with the government of the third country, territory or processing sector within that third country or the international organisation.

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

8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until ***five years after the entry into force of this Regulation unless amended, replaced or repealed by the Commission before the end of this period***.

Recitals

(80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector 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.***~~ ***The Commission may also decide, having given notice and a complete justification to the third country, to revoke such a decision.***

(81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country,

take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards.

(82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. ***Any legislation which provides for extra-territorial access to personal data processed in the Union without authorisation under Union or Member State law should be considered as an indication of a lack of adequacy.*** Consequently the transfer of personal data to that third country should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.

COMP AM Article 42
17.10.2013

Article 42
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 or processing sector 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. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:

(a) binding corporate rules in accordance with Article 43; or

(aa) a valid "European Data Protection Seal" for the controller and the recipient in accordance with paragraph 1e of Article 39;

~~***(b) standard data protection clauses adopted by the Commission after consulting the European Data Protection. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or***~~

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or

(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

3. A transfer based on standard data protection clauses***, a "European Data Protection Seal"*** or binding corporate rules as referred to in points (a), ***(aa)*** ~~***(b)***~~ or (c) of paragraph 2 shall not require any ~~further~~ ***specific*** authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5. ~~Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is~~

~~related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.~~ Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid~~,~~ until ***two years after the entry into force of this Regulation*** unless ***amended, replaced or repealed by that supervisory authority before the end of this period***.

Recitals

(83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority***~~, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority.~~ Those appropriate safeguards should uphold a respect of the data subject rights adequate to intra-EU processing, in particular relating to purpose limitation, right to access, rectification, erasure and to claim compensation. Those safeguards should in particular guarantee the observance of the principles of personal data processing, safeguard data subject rights and provide for effective redress mechanisms, ensure the observance of the principles of data protection by design and by default, guarantee the existence of a data protection officer.***

(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses ***or supplementary safeguards*** as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by ***~~the Commission or by~~*** a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. ***The standard data protection clauses adopted by the Commission could cover different situations, namely transfers from controllers established in the European Union to controllers established outside the European Union and from controllers established in the European Union to processors, including sub-processors, established outside the European Union. Controllers and processors should be encouraged to provide even more robust safeguards via additional contractual commitments that supplement standard protection clauses.***

COMP AM Article 43
07.10.2013

Article 43
Transfers by way of binding corporate rules

1. ~~*A*~~ ***The*** supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:

(a) are legally binding and apply to and are enforced by every member within the controller's ~~***or processor's***~~ group of undertakings ***and those external subcontractors that are covered by the scope of the binding corporate rules***, and include their employees;

(b) expressly confer enforceable rights on data subjects;

(c) fulfil the requirements laid down in paragraph 2.

1a. With regard to employment data, the representatives of the employees shall be informed about and, in accordance with Union or Member State law and practice, be involved in the drawing-up of binding corporate rules pursuant to Article 43.

2. The binding corporate rules shall at least specify:

(a) the structure and contact details of the group of undertakings and its members ***and those external subcontractors that are covered by the scope of the binding corporate rules***;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the general data protection principles, in particular purpose limitation, ***data minimisation, limited retention periods,*** data quality, ***data protection by design and by default,*** legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;

(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller ~~***or processor***~~ established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;

(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;

(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;

(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the ***format, procedures,*** criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, ***including transparency for data subjects,*** the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.

~~***4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted, after requesting an opinion of the European Data Protection Board, in accordance with the examination procedure set out in Article 87(2).***~~

Recitals

(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include ***all*** essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

COMP AM Article 43a
17.10.2013

Article 43a
Transfers or disclosures not authorised by Union law

1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.

2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer or disclosure by the supervisory authority.

3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with Article 44(1)(d) and (e) and (5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

4. The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subjects of the request and of the authorisation by the supervisory authority and where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1).

~~***5. The Commission may lay down the standard format of the notifications to the supervisory authority referred to in paragraph 2 and the information of the data subject referred to in paragraph 4 as well as the procedures applicable to the notification and information. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).***~~

Recitals

(90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act. ***In cases***

where controllers or processors are confronted with conflicting compliance requirements between the jurisdiction of the EU on the one hand, and that of a third country on the other, the Commission should ensure that EU law takes precedence at all times. The Commission should provide guidance and assistance to the controller and processor, and it should seek to resolve the jurisdictional conflict with the third country in question.

COMP AM Article 44
16.10.2013

Article 44
Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for important grounds of public interest; or

(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

~~(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.~~

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

~~3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of~~

~~*origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.*~~

4. Points (b)~~*,*~~ ***and*** (c) ~~***and (h)***~~ of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.

~~***6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.***~~

7. The ~~***Commission***~~ ***European Data Protection Board*** shall be ***entrusted with the task of issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b)*** ~~***empowered to adopt delegated acts in accordance with Article 86***~~ for the purpose of further specifying ~~***'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as***~~ the criteria and requirements for ~~***appropriate safeguards referred to in point (h)***~~ ***data transfers on the basis*** of paragraph 1.

Recitals

(86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients***, taking into full account the interests and fundamental rights of the data subject***.

(87) These derogations should in particular apply to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters ***or for public health,*** or to competent ***public*** authorities for the prevention, investigation, detection and prosecution of criminal offences***, including for the prevention of money laundering and the fight against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's life, if the data subject is incapable of giving consent. Transferring personal data for such important grounds of public interest should only be used for occasional transfers. In each and every case, a careful assessment of all circumstances of the transfer should be carried out.***

(88) ~~***Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when***~~

~~***they have assessed all the circumstances surrounding the data transfer.***~~ For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.

(89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a ***legally binding*** guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred***, to the extent that the processing is not massive, not repetitive and not structural***. ***That guarantee should include financial indemnification in cases of loss or unauthorised access or processing of the data and an obligation, regardless of national legislation, to provide full details of all access to the data by public authorities in the third country.***

COMP AM Article 45
14.10.2013

Article 45
International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities 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 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 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 41(3).

COMP AM Articles 45a
07.10.2013

Article 45a
Report by the Commission

The Commission shall submit to the European Parliament and the Council at regular intervals, starting not later than four years after the date referred to in Article 91(1), a report on the application of Articles 40 to 45. For that purpose, the Commission may request information from the Member States and supervisory authorities, which shall be supplied without undue delay. The report shall be made public.

COMP Article 46
7.10.2013

Chapter VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 1
INDEPENDENT STATUS

Article 46
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation 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 these purposes, the supervisory authorities shall co-operate with each other and the Commission.

2. Where in a Member State more than one supervisory authority are established, 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 and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article
57.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Recitals

(92) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection on individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. ***An authority shall have adequate financial and personal resources to fully carry out its role, taking into account the size of the population and the amount of personal data processing.***

(93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.

COMP Article 47
14.10.2013

Article 47
Independence

1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it***, notwithstanding co-operation and consistency arrangements pursuant to Chapter VII of this Regulation***.

2. The members of the supervisory authority shall, 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 participation in the European Data Protection Board.

6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be 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.

7a. Each Member State shall ensure that the supervisory authority shall be accountable to the national parliament for reasons of budgetary control.

COMP Article 48
7.10.2013

Article 48
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 notably in the area of protection of personal data 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 fulfills 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 the duties until a new member is appointed.

Recitals

(95) 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 appointed by the parliament or the government of the Member State ***taking due care to minimise the possibility of political interference***, and include rules on the personal qualification of the members***, the avoidance of conflicts of interest*** and the position of those members.

COMP Article 49
7.10.2013

Article 49
Rules on the establishment of the supervisory authority

Each Member State shall provide by law within the limits of this Regulation:

(a) the establishment and status of the supervisory authority;

(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 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 Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(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 in case that they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.

COMP Article 50
7.10.2013

Article 50
Professional secrecy

The members and the staff of the supervisory authority shall be 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 the Regulation***.

COMP AM Article 51
14.10.2013

Chapter VI
INDEPENDENT SUPERVISORY AUTHORITIES

SECTION 2
DUTIES AND POWERS

Article 51
Competence

1. Each supervisory authority shall be ***competent to perform the duties and to*** exercise~~***, on the territory of its own Member State,***~~ the powers conferred on it in accordance with this Regulation ***on the territory of its own Member State, without prejudice to Articles 73 and 74***. ***Data processing by a public authority shall be supervised only by the supervisory authority of that Member State.***

~~***2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.***~~

3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Recitals

(96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.

(99) While this Regulation applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when courts 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 strictly limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in, in accordance with national law.

COMP AM Article 52
15.10.2013

Article 52
Duties

1. The supervisory authority shall:

(a) monitor and ensure the application of this Regulation;

(b) hear complaints lodged by any data subject, or by an association ***~~representing that data subject~~*** in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;

(d) conduct investigations, either on its own initiative or on the basis of a complaint or ***of specific and documented information received alleging unlawful processing or*** on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period;

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

(f) be 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;

(g) authorise and be consulted on the processing operations referred to in Article 34;

(h) issue an opinion on the draft codes of conduct pursuant to Article 38(2);

(i) approve binding corporate rules pursuant to Article 43;

(j) participate in the activities of the European Data Protection Board***;***

(ja) certify controllers and processors pursuant to Article 39.

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 ***and on appropriate measures for personal data protection***. Activities addressed specifically to children shall receive specific attention.

2a. Each supervisory authority shall together with the European Data Protection Board promote the awareness of controllers and processors on risks, rules, safeguards and rights in relation to the processing of personal data. This includes keeping a register of sanctions and breaches. The register should enroll both all warnings and sanctions as detailed as possible, and the resolving of breaches. Each supervisory authority shall provide micro, small and medium sized enterprise controllers and processors on request with general information on their responsibilities and obligations in accordance with this Regulation.

3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation 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. The performance of the duties of the supervisory authority shall be free of charge for the data subject.

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

Recitals

(100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity with Union law and national law. This concerns in particular the requirement to obtain a prior judicial authorisation.

(101) Each supervisory authority should hear complaints lodged by any data subject ***or by an association acting in the public interest*** 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 ***or the association*** 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.

(102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.

COMP AM Article 53
16.10.2013

Article 53
Powers

1. Each supervisory authority shall***, in line with this regulation,*** have 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, ***or to order the controller to communicate a personal data breach to the data subject***;

(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;

(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;

(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;

(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 of this Regulation 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 issue opinions on any issue related to the protection of personal data;

(ia) to certify controllers and processors pursuant to Article 39;

(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.

(ja) to put in place effective mechanisms to encourage confidential reporting of breaches of this Regulation, taking into account guidance issued by the European Data Protection Board pursuant to Article 66(4b).

2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor ***without prior notice***:

(a) access to all personal data and to all ***documents and*** information necessary for the performance of its duties;

(b) access to any of its premises, including to any data processing equipment and means, ~~***where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there***~~.

The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.

3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).

4. Each supervisory authority shall have the power to sanction administrative offences, in ***accordance with*** ~~***particular those referred to in***~~ Article 79~~***(4), (5) and (6)***~~. ***This power shall be exercised in an effective, proportionate and dissuasive manner.***

COMP AM Article 54
07.10.2013

Article 54
Activity report

Each supervisory authority must draw up ***a ~~an annual~~*** report on its activities ***at least every two years***. The report shall be presented to the ***respective ~~national~~*** parliament and shall be made be available to the public, the Commission and the European Data Protection Board.

COMP AM Article 54a
17.10.2013

CHAPTER VII
CO-OPERATION AND CONSISTENCY

SECTION 1
CO-OPERATION

Article 54a
Lead Authority

1. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State***, or where personal data of the residents of several Member States are processed,*** the supervisory authority of the main establishment of the controller or processor shall ***act as the lead authority responsible*** ~~***be competent***~~ for the supervision of the processing activities of the controller or the processor in all Member States, ***in accordance with*** ~~***without prejudice to***~~ the provisions of Chapter VII of this Regulation.

2. The lead supervisory authority shall take appropriate measures for the supervision of the processing activities of the controller or processor for which it is responsible only after consulting all other competent supervisory authorities within the meaning of paragraph 1 of Article 51 in an endeavour to reach a consensus. For that purpose it shall in particular submit any relevant information and consult the other authorities before it adopts a measure intended to produce legal effects vis-à-vis a controller or a processor within the meaning of paragraph 1 of Article 51. The lead authority shall take the utmost account of the opinions of the authorities involved. The lead authority shall be the sole authority empowered to decide on measures intended to produce legal effects as regards the processing activities of the controller or processor for which it is responsible.

3. The European Data Protection Board shall, at the request of a competent supervisory authority, issue an opinion on the identification of the lead authority responsible for a controller or processor, in cases where:
(a) it is unclear from the facts of the case where the main establishment of the controller or processor is located; or
(b) the competent authorities do not agree on which supervisory authority shall act as lead authority;
(c) the controller is not established in the Union, and residents of different Member States are affected by processing operations within the scope of this Regulation.

3a. Where the controller exercises also activities as a processor, the supervisory authority of the main establishment of the controller shall act as lead authority for the supervision of processing activities.

4. The European Data Protection Board may decide on the identification of the lead authority.

Recitals

(97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should ***act as the single contact point and the lead authority responsible for supervising*** the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.

(98) The ***lead*** authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment or its representative. ***The European Data Protection Board may designate the lead authority through the consistency mechanism in certain cases on the request of a competent authority.***

(98a) Data subjects whose personal data is processed by a data controller or processor in another Member State should be able to complain to the supervisory authority of their choice. The lead data protection authority should coordinate its work with that of the other authorities involved.

COMP AM Article 55
07.10.2013

Article 55
Mutual Assistance

1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation 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 authorisations and consultations, inspections ***and investigations*** and prompt information on the opening of cases and ensuing developments ***where the controller or processor has establishments in several Member States or*** where data subjects in several Member States are likely to be affected by processing operations. ***The lead authority as defined in Article 54a shall ensure the coordination with involved supervisory authorities and shall act as the single contact point for the controller or processor.***

2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.

3. 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.

4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:

(a) it is not competent for the request; or

(b) compliance with the request would be incompatible with the provisions of this Regulation.

5. 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.

6. 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.

7. No fee shall be charged ***to the requesting supervisory authority*** for any action taken following a request for mutual assistance.

8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and

shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57. ***Where no definitive measure is yet possible because the assistance is not yet completed, the requesting supervisory authority may take interim measures under Article 53 in the territory of its Member State***.

9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission ***in accordance with the procedure referred to in Article 57***.

10. The ***European Data Protection Board*** ~~***Commission***~~ may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. ~~***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).***~~

Recitals

(103) The supervisory authorities should assist each other in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.

COMP AM Article 56
07.10.2013

Article 56
Joint operations of supervisory authorities

1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved.

2. In cases ***where the controller or processor has establishments in several Member States or*** where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint operations, as appropriate. The ***lead authority as defined in Article 54a*** ~~***competent authority***~~ shall ***involve*** ~~***invite***~~ the supervisory authority of each of those Member States ~~***to take part***~~ in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay. ***The lead authority shall act as the single contact point for the controller or processor.***

3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their executive powers in accordance with the seconding supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.

4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions.

5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1).

6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.

Recitals

(104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.

COMP AM Article 57
07.10.2013

SECTION 2
CONSISTENCY

Article 57
Consistency mechanism

For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism ***both on matters of general scope and in individual cases in accordance with the provisions of*** ~~***as set out***~~ this section.

Recitals

(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, or to the monitoring ***of*** such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. ***Furthermore, the data subjects should have the right to obtain consistency, if they deem a measure by a Data Protection Authority of a Member State has not fulfilled this criterion***. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

COMP AM Article 58
14.10.2013

Article 58
Consistency on matters of general application ~~***Opinion by the European Data Protection Board***~~

1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:

~~***(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or***~~

~~***(b) may substantially affect the free movement of personal data within the Union; or***~~

~~***(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or***~~

(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or

(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or

(f) aims to approve binding corporate rules within the meaning of Article 43.

3. Any supervisory authority or the European Data Protection Board may request that any matter ***of general application*** shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter ***of general application*** shall be dealt with in the consistency mechanism.

5. Supervisory authorities and the Commission shall ***without undue delay*** ~~***immediately***~~ electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.

6. The chair of the European Data Protection Board shall ***without undue delay*** ~~***immediately***~~ electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a

standardised format. The secretariat of the European Data Protection Board shall provide translations of relevant information, where necessary.

6a. The European Data Protection Board shall adopt an opinion on matters referred to it under paragraph 2.

7. The European Data Protection Board ~~***shall***~~ ***may decide by simple majority whether to*** adopt an opinion on ***any*** ~~***the***~~ ***matter submitted under paragraphs 3 and 4 taking into account*** ~~***if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.:***~~

(a) whether the matter presents elements of novelty, taking account of legal or factual developments, in particular in information technology and in the light of the state of progress in the information society; and

(b) whether the European Data Protection Board has already issued an opinion on the same matter.

8. ***The European Data Protection Board shall adopt opinions pursuant to paragraphs 6a and 7 by a simple majority of its members. These opinions shall be made public.*** ~~***The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.***~~

Recitals

(106) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a simple majority of its members so decides or if so requested by any supervisory authority or the Commission.

COMP AM Article 58a
07.10.2013

Article 58a
Consistency in individual cases

1. Before taking a measure intended to produce legal effects within the meaning of Article 54a, the lead authority shall share all relevant information and submit the draft measure to all other competent authorities. The lead authority shall not adopt the measure if a competent authority has, within a period of three weeks, indicated it has serious objections to the measure.

2. Where a competent authority has indicated that it has serious objections to a draft measure of the lead authority, or where the lead authority does not submit a draft measure referred to in paragraph 1 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56, the issue shall be considered by the European Data Protection Board.

3. The lead authority and/or other competent authorities involved and the Commission shall without undue delay electronically communicate to the European Data Protection Board using a standardised format any relevant information, including as the case may be a summary of the facts, the draft measure, the grounds which make the enactment of such measure necessary, the objections raised against it and the views of other supervisory authorities concerned.

4. The European Data Protection Board shall consider the issue, taking into account the impact of the draft measure of the lead authority on the fundamental rights and freedoms of data subjects, and shall decide by simple majority of its members whether to issue an opinion on the matter within two weeks after the relevant information has been provided pursuant to paragraph 3.

5. In case the European Data Protection Board decides to issue an opinion, it shall do so within six weeks and make the opinion public.

6. The lead authority shall take utmost account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format. Where the lead authority intends not to follow the opinion of the European Data Protection Board, it shall provide a reasoned justification.

7. In case the European Data Protection Board still objects to the measure of the supervisory authority as referred to in paragraph 5, it may within one month adopt by a two thirds majority a measure which shall be binding upon the supervisory authority.

<u>Recitals</u>

(106a) In order to ensure the consistent application of this Regulation, the European Data Protection Board may in individual cases adopt a decision which is binding on the competent supervisory authorities.

COMP AM Article 59
07.10.2013

~~*Article 59*~~
~~*Opinion by the Commission*~~

~~*1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.*~~

~~*2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.*~~

~~*3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.*~~

~~*4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.*~~

Recitals

~~*(107) In order to ensure compliance with this Regulation, the Commission may adopt an opinion on this matter, or a decision, requiring the supervisory authority to suspend its draft measure.*~~

COMP AM Article 60
07.10.2013

~~*Article 60*~~
~~*Suspension of a draft measure*~~

~~*1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:*~~
~~*(a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or*~~
~~*(b) adopt a measure pursuant to point (a) of Article 62(1).*~~

~~*2. The Commission shall specify the duration of the suspension which shall not exceed 12 months.*~~

~~*3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.*~~

COMP AM Article 60a
07.10.2013

Article 60a
Notification of Parliament and Council

The Commission shall notify the Council and the European Parliament at regular intervals, at least every two years, on the basis of a report from the Chair of the European Data Protection Board, of the matters dealt with under the consistency procedure, setting out the conclusions drawn by the Commission and the European Data Protection Board with a view to ensuring the consistent implementation and application of this regulation.

COMP AM Article 61
07.10.2013

Article 61
Urgency procedure

1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article ***58a*** ~~***57***~~, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.

3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.

4. ~~***By derogation from Article 58(7), an***~~ ***An*** urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.

Recitals

(108) There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.

COMP AM Article 62
16.10.2013

Article 62
Implementing Acts

1. The Commission may adopt implementing acts ***of general application***, ***after requesting an opinion of the European Data Protection Board,*** for:

~~***(a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;***~~

(b) deciding~~***, within the period referred to in Article 59(1),***~~ whether it declares draft standard data protection clauses referred to in point (d) of Article ***42*** ~~***58***~~(2), as having general validity;

~~***(c) specifying the format and procedures for the application of the consistency mechanism referred to in this section;***~~

(d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8).

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

~~***2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.***~~

3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.

COMP AM Article 63
07.10.2013

Article 63
Enforcement

1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.

2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) ***and (2) ~~to (5)~~ or adopts a measure despite an indication of serious objection pursuant to Article 58a(1)***, the measure of the supervisory authority shall not be legally valid and enforceable.

Recitals

(109) The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.

COMP AM Article 64
14.10.2013

CHAPTER VII
CO-OPERATION AND CONSISTENCY

SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 64
European Data Protection Board

1. A European Data Protection Board is hereby set up.

2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.

3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.

4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.

Recitals

(110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the ***institutions of the Union*** ~~***Commission***~~ and promoting cooperation of the supervisory authorities throughout the Union***, including the coordination of joint operations***. The European Data Protection Board should act independently when exercising its tasks. ***The European Data Protection Board should strengthen the dialogue with concerned stakeholders such as data subjects' associations, consumer organisations, data controllers and other relevant stakeholders and experts.***

COMP AM Article 65
07.10.2013

Article 65
Independence

1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67.

2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.

COMP AM Article 66
14.10.2013

Article 66
Tasks of the European Data Protection Board

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the ***European Parliament, Council or*** Commission, in particular:

(a) advise the ***European Institutions*** ~~***Commission***~~ on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

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

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

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;

(da) provide an opinion on which authority should be the lead authority pursuant to Article 54a(3);

(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 several 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 on data protection legislation and practice with data protection supervisory authorities worldwide.

(ga) give its opinion to the Commission in the preparation of delegated and implementing acts based on this Regulation;

(gb) give its opinion on codes of conduct drawn up at Union level pursuant to Article 38(4);

(gc) give its opinion on criteria and requirements for the data protection certification mechanisms pursuant to Article 39(9).

(gd) maintain a public electronic register on valid and invalid certificates pursuant to Article 39(8);

(ge) provide assistance to a national supervisory authorities, at their request;

(gf) establish and make public a list of the processing operations which are subject to prior consultation pursuant to Article 34;

(gg) maintain a registry of sanctions imposed on controllers or processors by the competent supervisory authorities.

2. Where the ***European Parliament, Council or*** 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 ***European Parliament, Council and*** Commission and to the committee referred to in Article 87 and make them public.

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

4a. The European Data Protection Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.

4b. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with paragraph 1 (b) for establishing common procedures for receiving and investigating information concerning allegations of unlawful processing and for safeguarding confidentiality and sources of information received.

COMP AM Article 67
07.10.2013

Article 67
Reports

1. The European Data Protection Board shall regularly and timely inform the ***European Parliament, Council and*** Commission about the outcome of its activities. It shall draw up ~~***an annual***~~ ***a*** report ***at least every two years*** on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries. The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).

2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.

COMP AM Article 68
07.10.2013

Article 68
Procedure

1. The European Data Protection Board shall take decisions by a simple majority of its members***, unless otherwise provided in its rules of procedure***.

2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.

COMP AM Article 69
07.10.2013

Article 69
Chair

1. The European Data Protection Board shall elect a chair and ***at least*** two deputy chairpersons from amongst its members. ~~***One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair.***~~

2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable.

2a. The position of the chair shall be a full-time position.

COMP AM Article 70
07.10.2013

Article 70
Tasks of the chair

1. The chair shall have the following tasks:
(a) to convene the meetings of the European Data Protection Board and prepare its agenda;
(b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.

2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.

COMP AM Article 71
07.10.2013

Article 71
Secretariat

1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat.

2. The secretariat shall provide analytical, ***legal,*** administrative and logistical support to the European Data Protection Board under the direction of the chair.

3. The secretariat shall be responsible in particular for:
(a) the day-to-day business of the European Data Protection Board;
(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;
(c) the use of electronic means for the internal and external communication;
(d) the translation of relevant information;
(e) the preparation and follow-up of the meetings of the European Data Protection Board;
(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.

COMP AM Article 72
07.10.2013

Article 72
Confidentiality

1. The discussions of the European Data Protection Board ***may ~~shall~~*** be confidential ***where necessary, unless otherwise provided in the rules of procedure***. ***The agendas of the meetings of the Board shall be made public***.

2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.

3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.

COMP AM Article 73
14.10.2013

CHAPTER VIII
REMEDIES, LIABILITY AND SANCTIONS

Article 73
Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy ***and the consistency mechanism***, every data subject shall have the right 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 this Regulation.

2. Any body, organisation or association which ~~***aims to protect data subjects' rights and interests concerning the protection of their personal data***~~ ***acts in the public interest*** and has been properly constituted according to the law of a Member State shall have the right 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 Regulation have been infringed as a result of the processing of personal data.

3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that ~~***a personal data***~~ breach ***of this regulation*** has occurred.

Recitals

(111) ~~***Every***~~ data subject***s*** should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a***n effective*** judicial remedy ***in accordance with Article 47 of the Charter of Fundamental Rights*** if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject.

(112) Any body, organisation or association which ~~***aims to protects the rights and interests of data subjects in relation to the protection of their data***~~ ***acts in the public interest*** and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority ***on behalf of data subjects with their consent*** or exercise the right to a judicial remedy ***if mandated by the*** ~~***on behalf of***~~ data subject~~***s***~~, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a ~~***personal data***~~ breach ***of this Regulation*** has occurred.

COMP AM Article 74
14.10.2013

Article 74
Right to a judicial remedy against a supervisory authority

1. ***Without prejudice to any other administrative or non-judicial remedy,*** each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.

2. ***Without prejudice to any other administrative or non-judicial remedy,*** each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision 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 52(1).

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. ***Without prejudice to the consistency mechanism a*** ~~A~~ data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.

5. The Member States shall enforce final decisions by the courts referred to in this Article.

Recitals

(113) 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.

(114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may ***mandate*** any body, organisation or association ~~***aiming to protect the rights and interests of data subjects in relation to the protection of their data***~~ ***acting in the public interest*** to bring proceedings against that supervisory authority to the competent court in the other Member State.

(115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. ***This does not apply to non-EU-residents.*** The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.

COMP AM Article 75
08.10.2013

Article 75
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 as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority ***of the Union or a Member State*** acting in the exercise of its public powers.

3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.

4. The Member States shall enforce final decisions by the courts referred to in this Article.

Recitals

(116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or***, in case of EU residence,*** where the data subject resides, unless the controller is a public authority ***of the Union or a Member State*** acting in the exercise of its public powers.

(117) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. Member States should ensure that court actions, in order to be effective, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.

COMP AM Article 76
08.10.2013

Article 76
Common rules for court proceedings

1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74***, ~~and~~*** 75 ***and 77 ~~on behalf of~~ if mandated by*** one or more data subjects.

2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.

3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.

4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.

5. 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.

COMP AM Article 77
14.10.2013

Article 77
Right to compensation and liability

1. Any person who has suffered damage***, including non-pecuniary damage,*** as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to ~~***receive***~~ ***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 ***of those*** controller***s*** or processor***s*** shall be jointly and severally liable for the entire amount of the damage***, unless they have an appropriate written agreement*** ~~***establishing liability in the determination of***~~ ***determining the responsibilities pursuant to Article 24***.

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

Recitals

(118) Any damage***, whether pecuniary or not,*** 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 ***only*** if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure.

COMP AM Article 78
08.10.2013

Article 78
Penalties

1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive. ~~***The rules on penalties adopted in accordance with this Article shall be subject to appropriate procedural safeguards in conformity with the general principles of Union law and the Charter of Fundamental Rights, including those concerning the right to an effective judicial remedy, due process and the principle of ne bis in idem.***~~

2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Recitals

(119) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties. ***The rules on penalties should be subject to appropriate procedural safeguards in conformity with the general principles of Union law and the Charter of Fundamental Rights, including those concerning the right to an effective judicial remedy, due process and the principle of ne bis in idem.***

(119a) In applying penalties, Member States should show full respect for appropriate procedural safeguards, including the right to an effective judicial remedy, due process, and the principle of ne bis in idem.

(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.

COMP Article 79
17.10.2013

Article 79
Administrative sanctions

1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. ***The supervisory authorities shall co-operate with each other in accordance with Articles 46 and 57 to guarantee a harmonized level of sanctions within the Union.***

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. ~~***The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.***~~

2a. To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:
a) a warning in writing in cases of first and non-intentional non-compliance;
b) regular periodic data protection audits;
c) a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater.

2b. If the controller or the processor is in possession of a valid "European Data Protection Seal" pursuant to Article 39, a fine pursuant to paragraph 2a(c) shall only be imposed in cases of intentional or negligent incompliance.

2c. The administrative sanction shall take into account the following factors:
a) the nature, gravity and duration of the incompliance,
b) the intentional or negligent character of the infringement,
c) the degree of responsibility of the natural or legal person and of previous breaches by this person,
d) the repetitive nature of the infringement,
e) the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement,
f) the specific categories of personal data affected by the infringement,
(fa) the level of damage, including non-pecuniary damage, suffered by the data subjects,
(fb) the action taken by the controller or processor to mitigate the damage suffered by data subjects,
(fc) any financial benefits intended or gained, or losses avoided, directly or indirectly from the infringement,
g) the degree of technical and organisational measures and procedures implemented pursuant to:
- ***i) Article 23 - Data protection by design and by default***
- ***ii) Article 30 - Security of processing***
- ***iii) Article 33 - Data protection impact assessment***

iv) Article 33 a (new) - Data protection compliance review
v) Article 35 - Designation of the data protection officer
(ga) the refusal to cooperate with or obstruction of inspections, audits and controls carried out by the supervisory authority pursuant to Article 53,
(gb) other aggravating or mitigating factors applicable to the circumstance of the case.

~~*3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:*~~
~~*(a) a natural person is processing personal data without a commercial interest; or*~~
~~*(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.*~~

~~*4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:*~~
~~*(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);*~~
~~*(a) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).*~~

~~*5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:*~~
~~*(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;*~~
~~*(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;*~~
~~*(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;*~~
~~*(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;*~~
~~*(e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;*~~
~~*(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);*~~
~~*(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.*~~

~~*6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:*~~
~~*(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;*~~
~~*(b) processes special categories of data in violation of Articles 9 and 81;*~~

~~***(c) does not comply with an objection or the requirement pursuant to Article 19;***~~
~~***(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;***~~
~~***(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;***~~
~~***(f) does not designate a representative pursuant to Article 25;***~~
~~***(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;***~~
~~***(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;***~~
~~***(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;***~~
~~***(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;***~~
~~***(k) misuses a data protection seal or mark in the meaning of Article 39;***~~
~~***(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;***~~
~~***(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);***~~
~~***(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);***~~
~~***(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.***~~

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the ***absolute*** amounts of the administrative fines referred to in paragraph~~***s 2a 4, 5 and 6***~~, taking into account the criteria ***and factors*** referred to in paragraph***s*** 2 ***and 2c***.

Recitals

(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.

COMP AM Article 80
15.10.2013

Article 80
Processing of personal data and freedom of expression

1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI, ~~***and***~~ on co-operation and consistency in Chapter VII ***and specific data processing situations in Chapter IX whenever this is necessary*** ~~***for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression***~~ in order to reconcile the right to the protection of personal data with the rules governing freedom of expression ***in accordance with the Charter of Fundamental Rights of the European Union***.

2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.

Recitals

(121) ***Whenever necessary, exemptions or derogations*** ~~***The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption***~~ from the requirements of certain provisions of this Regulation for the processing of personal data ***should be provided for*** in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. ~~***This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries.***~~ Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities***,*** ~~***and***~~ on co-operation and consistency***, and on specific data processing situations***. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom~~***, such as journalism,***~~ broadly ~~***Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of***~~ ***to cover all these*** activities ***which aim at is*** the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them, ***also taking into account technological development***. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

COMP Article 80a
7.10.2013

Article 80a
Access to documents

1. Personal data in documents held by a public authority or a public body may be disclosed by this authority or body in accordance with Union or Member State legislation regarding public access to official documents, which reconciles the right to the protection of personal data with the principle of public access to official documents.

2. Each Member State shall notify to the Commission provisions of its law which it adopts pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Recitals

(18) This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. ***Personal data in documents held by a public authority or public body may be disclosed by that authority or body in accordance with Union or Member State law regarding public access to official documents, which reconciles the right to data protection with the right of public access to official documents and constitutes a fair balance of the various interests involved***.

COMP Article 81
16.10.2013

Article 81
Processing of personal data concerning health

1. ~~***Within the limits of***~~ ***In accordance with the rules set out in*** this Regulation, ~~***and in accordance***~~ ***in particular*** with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable, ***consistent,*** and specific measures to safeguard the data subject's ~~***legitimate***~~ interests ***and fundamental rights,*** to the extent that these are necessary ***and proportionate, and of which the effects shall be foreseeable by the data subject,*** for:

(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or

(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices, ***and if the processing is carried out by a person bound by a confidentiality obligation;*** or

(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system ***and the provision of health services. Such processing of personal data concerning health for reasons of public interest shall not result in data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.***

1a. When the purposes referred to in points (a) to (c) of paragraph 1 can be achieved without the use of personal data, such data shall not be used for those purposes, unless based on the consent of the data subject or Member State law.

1b. Where the data subject's consent is required for the processing of medical data exclusively for public health purposes of scientific research, the consent may be given for one or more specific and similar researches. However, the data subject may withdraw the consent at any time.

1c. For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Directive 2001/20/EC shall apply.

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes~~***, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is***~~ ***shall be permitted only with the consent of the data subject, and shall be*** subject to the conditions and safeguards referred to in Article 83.

2a. Member States law may provide for exceptions to the requirement of consent for research, as referred to in paragraph 2, with regard to research that serves a high public interests, if that research cannot possibly be carried out otherwise. The data in question shall be anonymised, or if that is not possible for the research purposes, pseudonymised under the highest technical standards, and all necessary measures shall be taken to prevent unwarranted re-identification of the data subjects. However, the data subject shall have the right to object at any time in accordance with Article 19.

3. The Commission shall be empowered to adopt, ***after requesting an opinion of the European Data Protection Board,*** delegated acts in accordance with Article 86 for the purpose of further specifying ~~***other reasons of***~~ public interest in the area of public health as referred to in point (b) of paragraph 1 ***and high public interest in the area of research as referred to in paragraph 2a~~, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1~~***.

3a. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Recitals

(122a) A professional who processes personal data concerning health should receive, if possible, anonymised or pseudonymised data, leaving the knowledge of the identity only to the General Practitioner or to the Specialist who has requested such data processing.

(123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that he alth status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. ~~***Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.***~~

(123a) The processing of personal data concerning health, as a special category of data, may be necessary for reasons of historical, statistical or scientific research. Therefore this Regulation foresees an exemption from the requirement of consent in cases of research that serves a high public interest.

COMP Article 82
16.10.2013

Article 82
Minimum standards for processing **data** in the employment context

1. Member States may, ***in accordance with the rules set out in this Regulation, and taking into account the principle of proportionality,*** adopt by ***~~law~~ legal provisions*** specific rules regulating the processing of employees' personal data in the employment context, in particular ***~~for~~ but not limited to*** the purposes of the recruitment ***and job applications within the group of undertakings,*** the performance of the contract of employment, including discharge of obligations, laid down by law ***and*** by collective agreements, ***in accordance with national law and practice,*** management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship. ***Member States may allow for collective agreements to further specify the provisions set out in this Article.***

1a. The purpose of processing such data must be linked to the reason it was collected for and stay within the context of employment. Profiling or use for secondary purposes shall not be allowed.

1b. Consent of an employee shall not provide a legal basis for the processing of data by the employer when the consent has not been given freely.

1c. Notwithstanding the other provisions of this Regulation, the legal provisions of Member States referred to in paragraph 1 shall include at least the following minimum standards:
(a) the processing of employee data without the employees' knowledge shall not be permitted. Notwithstanding sentence 1, Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the employee has committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the competent authority;
(b) the open optical-electronic and/or open acoustic-electronic monitoring of parts of an undertaking which are not accessible to the public and are used primarily by employees for private activities, especially in bathrooms, changing rooms, rest areas, and bedrooms, shall be prohibited. Clandestine surveillance shall be inadmissible under all circumstances;
(c) where undertakings or authorities collect and process personal data in the context of medical examinations and/or aptitude tests, they must explain to the applicant or employee beforehand the purpose for which these data are being used, and ensure that afterwards they are provided with these data together with the results, and that they receive an explanation of their significance on request. Data collection for the purpose of genetic testing and analyses shall be prohibited as a matter of principle;

(d) whether and to what extent the use of telephone, e-mail, internet and other telecommunications services shall also be permitted for private use may be regulated by collective agreement. Where there is no regulation by collective agreement, the employer shall reach an agreement on this matter directly with the employee. In so far as private use is permitted, the processing of accumulated traffic data shall be permitted in particular to ensure data security, to ensure the proper operation of telecommunications networks and telecommunications services and for billing purposes.
Notwithstanding sentence 3, Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the employee has committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the competent authority;
(e) workers' personal data, especially sensitive data such as political orientation and membership of and activities in trade unions, may under no circumstances be used to put workers on so-called 'blacklists', and to vet or bar them from future employment. The processing, the use in the employment context, the drawing-up and passing-on of blacklists of employees or other forms of discrimination shall be prohibited. Member States shall conduct checks and adopt adequate sanctions in accordance with Article 79(6) to ensure effective implementation of this point.

1d. Transmission and processing of personal employee data between legally independent undertakings within a group of undertakings and with professionals providing legal and tax advice shall be permitted, providing it is relevant to the operation of the business and is used for the conduct of specific operations or administrative procedures and is not contrary to the interests and fundamental rights of the person concerned which are worthy of protection. Where employee data are transmitted to a third country and/or to an international organization, Chapter V shall apply.

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to ***paragraphs 1 and 1b***, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

3. The Commission shall be empowered, ***after requesting an opinion from the European Data Protection Board,*** to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

Recital
(124) The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment ***and the social security*** context. ***Member States should be able*** to regulate the processing of employees' personal data in the employment ***and the processing of personal data in the social security*** context, ***in accordance with the rules and minimum standards set out in*** this Regulation***. Where a statutory basis is provided in the Member State in question for the regulation of employment matters by agreement between employee representatives and the management of the undertaking or the controlling undertaking of a group of undertakings (collective agreement) or under Directive 2009/38/EC of the European Parliament and of the Council***

of 6 May 2009 on the establishment of a European Works Council or a procedure in Community-scale undertakings and Community-scale groups of undertakings for the purposes of informing and consulting employees, the processing of personal data in ***an*** employment ***context may also be regulated by such an agreement.***

COMP Article 82a
7.10.2013

Article 82a
Processing in the social security context

1. Member States may, in accordance with the rules set out in this Regulation, adopt specific legislative rules particularising the conditions for the processing of personal data by their public and private institutions and departments in the social security context if carried out in the public interest.

2. Each Member State shall notify to the Commission those provisions which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and any subsequent amendment affecting them.

COMP Article 83
17.10.2013

Article 83
Processing for historical, statistical and scientific research purposes

1. ***In accordance with the rules set out in this Regulation***, personal data may be processed for historical, statistical or scientific research purposes only if:

(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information ~~***as long as these purposes can be fulfilled in this manner***~~ ***under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects.***

~~***2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:***~~
~~***(a) the data subject has given consent, subject to the conditions laid down in Article 7;***~~
~~***(b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or***~~
~~***(c) the data subject has made the data public.***~~

~~***3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.***~~

Recitals

(125) The processing of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as on clinical trials.

(126) Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area. ***The processing of personal data for historical, statistical and scientific research purposes should not result in personal data being processed for other purposes, unless with the consent of the data subject or on the basis of Union or Member State law.***

COMP Article 83a
7.10.2013

Article 83a
Processing of personal data by archive services

1. Once the initial processing for which they were collected has been completed, personal data may be processed by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest, in particular in order to substantiate individuals' rights or for historical, statistical or scientific research purposes. These tasks shall be carried out in accordance with the rules laid down by Member States concerning access to and the release and dissemination of administrative or archive documents and in accordance with the rules set out in this Regulation, specifically with regard to consent and the right to object.

2. Each Member State shall notify to the Commission provisions of its law which it adopts pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Recitals

(125a) Personal data may also be processed subsequently by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest. Member State legislation should reconcile the right to the protection of personal data with the rules on archives and on public access to administrative information. Member States should encourage the drafting, in particular by the European Archives Group, of rules to guarantee the confidentiality of data vis-à-vis third parties and the authenticity, integrity and proper conservation of data.

COMP Article 84
7.10.2013

Article 84
Obligations of secrecy

1. ***In accordance with the rules set out in*** this Regulation, Member States ***~~may adopt~~ shall ensure*** specific rules ***are in place setting ~~set~~*** out the ***~~investigative~~*** powers by the supervisory authorities laid down in Article 53***~~(2)~~*** in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Recitals

(127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.

COMP Article 85
14.10.2013

Article 85
Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, ~~***comprehensive***~~ ***adequate*** rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.

2. Churches and religious associations which apply ~~***comprehensive***~~ ***adequate*** rules in accordance with paragraph 1 shall ~~***provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation***~~ ***obtain a compliance opinion pursuant to Article 38***.

Recitals

(128) This Regulation respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, ~~***comprehensive***~~ ***adequate*** rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation ***and recognised as compliant***. ~~***Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.***~~

COMP Article 85a
10.10.2013

Article 85a
Respect of fundamental rights

This Regulation shall not have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the TEU.

Recital

(139) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.

COMP AM Article 85b (Beginning of Chapter X)
16.10.2013

Article 85b
Standard Forms

The Commission may, taking into account the specific features and necessities of various sectors and data processing situations, lay down standard forms for

a) specific methods to obtain verifiable consent referred to in Article 8(1),
b) the communication referred to in Article 12(2), including the electronic format,
c) providing the information referred to in paragraphs 1 to 3 of Article 14,
d) requesting and granting access to the information referred to in Article 15(1), including for communicating the personal data to the data subject,
e) documentation referred to in paragraph 1 of Article 28,
f) breach notifications pursuant to Article 31 to the supervisory authority and the documentation referred to in Article 31(4),
g) prior consultations referred to in Article 34, and for informing the supervisory authorities pursuant to Article 34(6).

2. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises.

3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Recitals

(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; 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; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. 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[1]. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(131) The examination procedure should be used for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access;, the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; 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; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism, given that those acts are of general scope.

(132) ~~***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 and relating to matters communicated by supervisory authorities under the consistency mechanism, imperative grounds of urgency so require.***~~
(technical amendment due to the changes in Article 44)

[1] 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 Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011, p. 13.

COMP AM Article 86
15.10.2013

Article 86
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 ***[Articles XXX]*** shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in ***[Articles XXX]*** 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 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 ***[Articles XXX]*** shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of ***six*** ~~***two***~~ 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*** ~~***two***~~ months at the initiative of the European Parliament or the Council.

COMP AM Article 87
10.10.2013

Article 87
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.***~~

COMP AM Article 88
14.10.2013

Article 88
Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Recitals

(133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout 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 Regulation does not go beyond what is necessary in order to achieve that objective.

(134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force. ***Commission decisions and authorisations by supervisory authorities relating to transfers of personal data to third countries pursuant to Article 41(8) should remain in force for a transition period of five years after the entry into force of this Regulation unless amended, replaced or repealed by the Commission before the end of this period.***

COMP Article 89
15.10.2013

Article 89
Relationship to and amendment of Directive 2002/58/EC

1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

2. Article***s*** 1(2)***, 4 and 15*** of Directive 2002/58/EC shall be deleted.

2a. The Commission shall present, without delay and by the date referred to in Article 91(2) at the latest, a proposal for the revision of the legal framework for the processing of personal data and the protection of privacy in electronic communications, in order to align the law with this regulation and ensure consistent and uniform legal provisions on the fundamental right to protection of personal data in the European Union.

Recitals

(135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly.

COMP Article 89a
7.10.2013

Article 89a
Relationship to and amendment of Regulation (EC) 2001/45

1. The rules set out in this Regulation shall be applied to the processing of personal data by Union institutions, bodies, offices and agencies in relation to matters for which they are not subject to additional rules set out in Regulation (EC) 2001/45.

2. The Commission shall present, without delay and by the date specified in Article 91(2) at the latest, a proposal for the revision of the legal framework applicable to the processing of personal data by the Union institutions, bodies, offices and agencies.

COMP Article 90
10.10.2013

Article 90
Evaluation

The Commission shall submit reports on the evaluation and review of this Regulation 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 Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society. The reports shall be made public.

COMP Article 91
9.10.2013

Article 91
Entry into force and application

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

2. It shall apply from [*two years from the date referred to in paragraph 1*].

This Regulation shall be binding in its entirety and directly applicable in all Member States.