

Brussels, 3 February 2015
(OR. en)

**Interinstitutional File:
2012/0011 (COD)**

17072/1/14
REV 1

LIMITE

**DATAPROTECT 189
JAI 1029
MI 1012
DRS 178
DAPIX 190
FREMP 233
COMIX 683
CODEC 2549**

NOTE

From: Presidency
To: Working Group on Information Exchange and Data Protection
Subject: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- Chapter II

Background

1. Following the discussions at the DAPIX meeting of 15-16 January 2016, the Presidency has made a number of further changes to the text of Chapter II, which are highlighted in the annex **in bold underlined text**.
2. Pending a revised version of the German proposal on consent (Article 7), the Presidency has chosen so far not to incorporate any of the suggestions made in that note¹.

¹ 14707/1/14 REV 1 DATAPROTECT 147 JAI 803 MI 806 DRS 136 DAPIX 151
FREMP 179 COMIX 569 CODEC 2087.

Specific questions

Further processing

3. Article 6, paragraphs 3a and 4, set out the regime for personal data that were initially processed for one purpose and subsequently processed for another purpose (further processing).

The Presidency has endeavored to make the following clarifications:

- only where the further purposes are incompatible with the initial purposes must a new legal basis be found;
- a new legal basis can also be found in a legitimate interest of the controller; and
- in case the new legal basis is a legitimate interest of the controller, the fact that those interests are incompatible with the initial grounds of processing as such does not prevent a controller from invoking such ground.

4. *Delegations are invited to confirm this understanding.*

Consent for children

5. Article 8 sets out a particular regime for consent for children, which are defined as minors below the age of fourteen years old. Paragraph 1 of this article requires consent to be given by parents and a new paragraph 1a completely rules out reliance on consent in some marketing cases. This draft article has given rise to a lot of discussion. A number of delegations have criticised this article which requires that the consent be expressed by the parent as being completely impossible to verify in practice and therefore impracticable. It has also been pointed out that this provision would bar public authorities or non-profit organisations like schools to rely on consent by children. Other delegations have argued that, in particular in the light of very worrying phenomena such as cyberbullying, the Union should take a principled stance. Reference has also been made to US legislation in this regard. Some delegations have also pleaded in favour of deleting this article, but beefing up some rights of data subjects in the context of Chapter III.

6. *Therefore delegations are invited to indicate:*

- *whether they want to maintain this article or delete it;*
- *in case it is kept, whether paragraph 1a should also be maintained;*
- *in case of deletion, whether they see the need to beef up some provisions in Chapter III;*
- *in case of deletion, whether -paragraph 1a on (direct) marketing should be kept or also deleted.*
- *in case the article is kept, which age should be set.*

International transfer of personal data of data concerning health

7. Article 9 (4a) concerns the case of an international transfer of personal data of data concerning health based on the vital interest when the data subject is unable to provide consent. One delegation has proposed that such transfer should be subjected to the condition that those data 'will be processed by a health professional subject to the obligation of professional secrecy under the law of the third State concerned or equivalent rules. Several delegations have opposed this proposal, indicating that this may lead to unacceptable situations where a data transfer will be - temporarily - blocked, whereas someone's vital interest, possible his or her life, is at stake.

8. *Therefore delegations are invited to indicate:*

- *whether they want to maintain this paragraph or delete it; and*
- *in case the paragraph is kept, it should stay in Article 9 or be moved to Chapter V.*

Processing of data relating to criminal convictions and offences

9. The Presidency has drafted an alternative to the current text which would clarify that the requirements laid down in this article are without prejudice to the use of other legal bases for processing this type of data and that the restrictions would not apply to these other legal bases. A variant would be to restrict this article to data on convictions and exclude criminal offences that have not yet lead to a conviction.

10. *Therefore delegations are invited to indicate:*

- *whether they prefer option 1 or 2; and*
- *whether the scope of the article should be confined to criminal convictions.*

23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Data including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes.

[The principles of data protection should not apply to deceased persons, unless information on deceased persons is related to an identified or identifiable natural person².]

23a) The application of pseudonymisation to personal data can reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations. The explicit introduction of ‘pseudonymisation’ through the articles of this Regulation is thus not intended to preclude any other measures of data protection.

23b) As a general rule personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. However, where further processing takes place by using measures of pseudonymisation, it should not be considered as incompatible with the purpose for which the data have been initially collected as long as the data subject is not identified or identifiable. Re-identification of pseudonymised personal data should require a separate legal basis.

² FR suggested this sentence be deleted.

- 23c) In order to create incentives for pseudonymisation, measures of pseudonymisation whilst allowing general analysis should be possible within the same controller when the controller has taken technical and organisational measures necessary to ensure that the provisions of this Regulation are implemented. The concrete requirements for those measures shall depend on the respective data processing so that the personal data remain pseudonymised. The controller who processes the data within the meaning of Art. 4 (3b) shall also refer to authorised persons within the same controller. In this case however the controller shall make sure that the individual(s) performing the pseudonymisation are not referenced in the meta-data³.**
- 24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. Identification numbers, location data, online identifiers or other specific factors as such should not (...) be considered as personal data (...) if they do not identify an individual or make an individual identifiable⁴.

³ Further to DE proposal.

⁴ DE reservation. ES, EE and IT also queried as regard the status of so-called identifiers. AT and SI thought the last sentence of the recital should be deleted. UK questioned whether so-called identifiers which were never used to trace back to a data subject should also be considered as personal data and hence subjected to the Regulation. It suggested stating that these can constitute personal data, but this will depend on the context. UK suggests deleting the words 'provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers' and 'received by the servers'. It also suggests deleting 'need not necessarily be considered as personal data in all circumstances' and replacing it by 'can constitute personal data, but this will depend on the context'. COM referred to the ECJ case law (Scarlett C-70/10) according to which IP addresses should be considered as personal data if they actually could lead to the identification of data subjects. DE queried who would in practice be responsible for such metadata.

25) Consent should be given unambiguously by any appropriate method enabling a freely-given, specific and informed indication of the data subject's wishes, either by a written, oral or other statement or by a clear affirmative action by the data subject signifying his or her agreement to personal data relating to him or her being processed. This could include ticking a box when visiting an Internet website or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Where it is technically feasible and effective, the data subject's consent to processing may be given by using the appropriate settings of a browser or other application. . **In such cases it is sufficient that the data subject receives the information needed to give informed consent when starting to use the service**⁵. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, unambiguous consent should be granted for all of the processing purposes. **It is often not possible to fully identify the purpose of data processing for scientific purposes at the time of data collection**. **Therefore it is necessary to ensure that consent may also cover as yet unknown issues while keeping with recognised ethical standards for scientific research, as has been the case in the past**. **Data subjects should have the opportunity to limit their consent to certain areas of research or parts of research projects to the extent allowed by the intended purpose and provided that this does not involve disproportionate efforts in view of the protective purpose**⁶. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

25a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.

⁵ DE proposal.

⁶ DE proposal.

- 26) Personal data concerning health should include (...) data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health of the data subject; including information about the registration of the individual for the provision of health services (...); a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (...) information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; (...) or any information on for example a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as for example from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.
- 27) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union. In this case the latter should be considered as the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes (...) and means of processing through stable arrangements. This criterion should not depend on whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union and, if it has no central administration in the Union, the place where the main processing activities take place in the Union⁷. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

⁷ Obviously this recital may need to be amended in the context of future discussion on the one-stop-shop principle.

- 28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.
- 29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. (...) ⁸.
- 30) Any processing of personal data should be lawful and fair. **The principle of fairness also means being able to use data within a free, open and social community reliant on communication and innovation, insofar as data subjects must accept this in the overriding public interest because of an individual's relatedness and connectedness to the community.** ⁹. It should be transparent for the individuals that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language is used. This concerns in particular the information of the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the individuals concerned and their right to get confirmation and communication of personal data being processed concerning them. Individuals should be made aware on risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise his or her rights in relation to the processing. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate and relevant (...) for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. (...). **Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review** ¹⁰. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or the use of personal data and the equipment used for the processing.

⁸ COM reservation on deletion of the reference to the UN Convention on the Rights of the Child.

⁹ DE proposal.

¹⁰ DE proposal.

- 31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate legal basis laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- 31a) Wherever this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant the constitutional order of the Member State concerned, however such legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it as required by the case law of the Court of Justice of the European Union and the European Court on Human Rights.
- 32) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that, and the extent to which, consent is given.
- For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended; consent should not be regarded as freely-given if the data subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment.
- 34) In order to safeguard that consent has been freely-given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and this imbalance makes it unlikely that consent was given freely in all the circumstances of that specific situation. (...)
- 35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.

- 35a) This Regulation provides for general rules on data protection and that in specific cases Member States are also empowered to lay down national rules on data protection. The Regulation does therefore not exclude Member State law that defines the circumstances of specific processing situations, including determining more precisely the conditions under which processing of personal data is lawful. National law may also provide for special processing conditions for specific sectors and for the processing of special categories of data.
- 36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a (...) basis in Union law or in the national law of a Member State. (...). It should be also for Union or national law to determine the purpose of the processing. Furthermore, this (...) basis could specify the general conditions of the Regulation¹¹ governing the lawfulness of data processing, determine specifications for determining the controller, the type of data which are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or by private law such as a professional association, where grounds of public interest so justify including for health purposes, such as public health and social protection and the management of health care services.
- 37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life or that of another person.

¹¹ DK would prefer to delete "of the Regulation" and refer simply to the general conditions.

- 38) The legitimate interests of a controller including of a controller to which the data may be disclosed may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. Legitimate interest could exist for example when there is a relevant and appropriate connection between the data subject and the controller in situations such as the data subject being a client or in the service of the controller. ¹²(...) The presence of a legitimate interest¹³ would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place. In particular such assessment must take into account whether the data subject is a child, given that children deserve specific protection. The data subject should have the right to object to the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. **(...)**
- 39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller *concerned*. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes can be regarded as carried out for a legitimate interest.¹⁴

¹² New drafting suggestion in order to ally the concerns of those Member States that thought the concept of legitimate interests should not be circumscribed (BE, DE, FR, IE).

¹³ Further to FI proposal.

¹⁴ AT was opposed to the reference on direct marketing. UK thought that this recital should also contain a reference to the use of pseudonymous data.

40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, **in which case no separate legal basis is required other than the one which allowed the collection of the data. Thus the further** processing (...) for **archiving purposes in the public interest or**, statistical, scientific or historical (...) purposes¹⁵ **is allowed without the need for another legal basis than the one for the initial collection of the personal data. Also further processing personal data for compliance with a legal obligation or in view of future dispute resolution**¹⁶ **and further processing personal data for reporting possible criminal behaviour should equally be considered as grounds which constitute compatible lawful processing operations**¹⁷ In order to ascertain whether a purpose of further processing is compatible with the purpose for which the data are initially collected, the controller, **after having met all the requirements for the lawfulness of the original processing**¹⁸, should take into account any link between those purposes and the purposes of the intended further processing, the context in which the data have been collected, including the reasonable expectations of the data subject as to their further use, the nature of the personal data, the consequences of the intended further processing for data subjects, and **the existence of appropriate safeguards in both the original and intended processing operations**¹⁹. Where the intended other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. **The provision is not intended to hinder legitimate business models such as direct marketing, debt collection or credit information services.** In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured. . **Further processing of personal data by the controller, notably transmitting personal data to competent authorities for public security purposes or other purposes pursuant to Art 2 para 2 lit. e, which are not required by a legal obligation or any other legal bases in Art. 6 para 1 lit. a to e should be regarded as a legitimate interest pursued by the controller**²⁰.

¹⁵ SE suggested to delete the last part of this sentence.

¹⁶ Further to NL proposal.

¹⁷ Further to DE proposal.

¹⁸ NL proposal.

¹⁹ NL proposal.

²⁰ DE proposal.

Further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.²¹

40b) Processing for a task assigned to an authority through Member State law with regard to Article 6(3) is generally deemed compatible if the respective purposes fall within the scope of the assigned task and the respective authority would also be authorised to collect the data for the other purpose too²².

- 41) Personal data which are, by their nature, particularly sensitive (...) in relation to fundamental rights and freedoms, deserve specific protection as the context of their processing may create important risks for the fundamental rights and freedoms. These data should also include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless processing is allowed in specific cases set out in this Regulation. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly be provided for where the data subject gives his or her explicit consent or in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms. Member State and Union Law may provide that the general prohibition for processing such special categories of personal data in certain cases may not be lifted by the data subject’s explicit consent²³.

²¹ UK queried the last sentence of recital 41, which was not reflected in the body of the text. DE, supported by GR, wanted it to be made clear that Article 6 did not hamper direct marketing or credit information services or businesses in general according to EL.

²² DE proposal.

²³ MT reservation on recitals 40 and 41.

42) Derogating from the prohibition on processing sensitive categories of data should also be allowed when provided for in Union or Member State law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where (...) grounds of public interest so justify, ***in particular processing data for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious (...) threats to health or ensuring high standards of quality and safety of health care and services and of medicinal products or medical devices or assessing public policies adopted in the field of health, also by producing quality and activity indicators.*** This may (...) be done for health purposes, including public health (...) ²⁴ and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for ***archiving in the public interest or*** historical, statistical and scientific (...) purposes.

A derogation should also allow processing of such data where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure.

42a) *Special categories of personal data which deserve higher protection, may only be processed for health-related purposes where necessary to achieve those purposes for the benefit of individuals and society as a whole, in particular in the context of the management of health-care services and systems including the processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health care system* ²⁵, *and ensuring continuity of health-care and cross-border healthcare or health security, monitoring and alert purposes or for archiving, historical, statistical or scientific purposes as well as for studies conducted in the public interest in the area of public health.* Therefore this Regulation should provide for harmonised conditions for the processing of *special categories of personal data concerning health, in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy* ²⁶ (...). Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of individuals. (...) ²⁷.

²⁴ The reference to social protection was deleted at the request of FR.

²⁵ DK proposal.

²⁶ UK preferred the term 'confidentiality', but this does not appear to be the correct term for professional secrecy imposed by legal or deontological rules.

²⁷ Moved from recitals 122.

- 42b) *The processing of special categories personal data (...) may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. This processing is subject to for suitable and specific measures so as to protect the rights and freedoms of individuals. 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 health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. 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 companies²⁸.*
- 43) Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.
- 44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.
- 45) If the data processed by a controller do not permit the controller to identify a natural person (...) the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. (...). However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights.

²⁸ Moved from recitals 123.

HAVE ADOPTED THIS REGULATION:

Article 4

Definitions

- (3b) 'pseudonymisation' means the processing of personal data by the controller in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person[, or can be attributed to such person only with the investment of a disproportionate amount of time, expense and manpower²⁹].

CHAPTER II

PRINCIPLES³⁰

Article 5

Principles relating to personal data processing³¹

1. Personal data must be:
 - (a) processed lawfully, fairly³² and in a transparent manner in relation to the data subject;

²⁹ DE proposal

³⁰ DE and SI scrutiny reservations.

³¹ DE scrutiny reservation.

³² DE thought this concept should be detailed; COM pointed out this was already done in recital 30.

- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of personal data for archiving purposes in the public interest **or scientific, statistical or historical purposes shall in accordance with Article 83**³³ not be considered incompatible with the initial purposes³⁴;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are processed (...)³⁵;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, **especially by applying appropriate measures of pseudonymisation at the earliest possible stage**³⁶; personal data may be stored for longer periods insofar as the data will be processed (...) for archiving purposes in the public interest³⁷ **or scientific, statistical, or historical purposes purposes in accordance with Article 83** subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of data subject³⁸;

³³ This reference was requested by BE, IE, but opposed by ES.

³⁴ Referring to Article 6(2), DE queried whether this phrase implied that a change of the purpose of processing was always lawful in case of scientific processing, also in the absence of consent by the data subject. BG thought that the second part of the sentence was redundant in view of Article 6(2). BE queried whether the concept of compatible purposes was still a useful one.

³⁵ COM reservation on the deletion of the data minimisation principle. AT, DE, EE, HU and SI preferred to return to the initial COM wording, stating 'limited to the minimum necessary'. DE also suggested adding: "they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data".

³⁶ DE proposal

³⁷ BE, supported by IE, suggested to insert a reference to Article 83. ES opposed the BE suggestion. COM meant that it was necessary to maintain the reference to *public interest* as well.

³⁸ NL and SK scrutiny reservation. SK indicated that the case of private archiving was still not addressed. BE and SE thought the last part of this sentence should be deleted.

(ee) processed in a manner that ensures appropriate security (...) of the personal data.

(f) (...)³⁹

2. The controller shall be responsible for compliance with paragraph 1⁴⁰.

Article 6

Lawfulness of processing⁴¹

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

- (a) the data subject has given unambiguous⁴² consent to the processing of their personal data for one or more specific purposes⁴³;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject (...)⁴⁴;

³⁹ AT wondered whether a principle of digital autonomy should be added here.

⁴⁰ It was previously proposed to add '*also in case of personal data being processed on its behalf by a processor*', but further to suggestion from FR, this rule on liability may be dealt with in the context of Chapter VIII. FR thought para. 2 in its entirety could be moved to this Chapter.

⁴¹ DE, AT, PT, SI and SK scrutiny reservation.

⁴² FR, PL and COM reservation in relation to the deletion of 'explicit' in the definition of 'consent'; UK thought that the addition of 'unambiguous' was unjustified.

⁴³ RO scrutiny reservation. UK suggested reverting to the definition of consent in Article 2(h) of the 1995 Directive.

⁴⁴ UK preferred the wording of the 1995 Directive.

- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - (f) processing is necessary for the purposes of the legitimate interests⁴⁵ pursued by the controller or by a third party⁴⁶ except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (...) ^{47 48}.
2. Processing of personal data which is necessary for archiving purposes in the public interest, or for historical, statistical or scientific purposes shall be lawful subject also to the conditions and safeguards referred to in Article 83.
3. The basis for the processing referred to in points (c) and (e) of paragraph 1 must be established in accordance with:
- (a) Union law, or
 - (b) national law of the Member State to which the controller is subject.

The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia the general conditions governing the lawfulness of data processing by the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing, including for other specific processing situations as provided for in Chapter IX.

⁴⁵ FR scrutiny reservation.

⁴⁶ Reinstated at the request of BG, CZ, DE, ES, HU, IT, NL, PL, SE, SK and UK. COM, IE and PL reservation on this reinstatement. IE said that the controller was a third party, in any case, neither a definition nor obligations for them had been introduced.

⁴⁷ Deleted at the request of BE, CZ, DK, IE, MT, SE, SI, SK, PT and UK.: IT wanted to maintain the last sentence. FR scrutiny reservation.

⁴⁸ DK and FR regretted there was no longer a reference to purposes set out in Article 9(2) and thought that the link between Article 6 and 9 needed to be clarified. This was also stressed by BE, CZ, DK, ES, NL, and DE. BE suggested the following sentence: The processing of special categories of data shall only be lawful to the extent that Article 6 is respected."

- 3a. In order to ascertain whether a purpose of further processing is compatible with the one for which the data are initially collected, the controller shall take into account, **unless the data subject has given consent**⁴⁹, inter alia⁵⁰:
- (a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;
 - (b) the context in which the data have been collected;
 - (c) the nature of the personal data, **in particular whether special categories of personal data, pursuant to Article 9**⁵¹;
 - (d) the possible consequences of the intended further processing for data subjects;
 - (e) the existence of appropriate safeguards⁵².
4. **Only** where the purpose of further processing is incompatible with the one for which the personal data have been collected, the further processing must have a legal basis at least in one of the grounds referred to in [points (a) to (f)⁵³ of] paragraph 1^{54 55}. **Further processing for incompatible purposes on grounds of legitimate interests of the controller or a third party shall be lawful if these interests override the interests of the data subject**⁵⁶.
5. (...)

⁴⁹ NL proposal.

⁵⁰ DK, FI, NL, RO, SI and SE stressed the list should not be exhaustive. PT: add consent.

⁵¹ NL proposal.

⁵² BG, DE, SK and PL reservation: safeguards as such do not make further processing compatible. FR queried to which processing this criterion related: the initial or further processing.

⁵³ (f) was added further to the request by DK, ES, FR and NL. Cion, FI and IT pleaded for its deletion.

⁵⁴ DE, HU, NL and PT scrutiny reservation. PT thought paragraph 4 could be deleted. BE queried whether this allowed for a hidden 'opt-in', e.g. regarding direct marketing operations, which COM referred to in recital 40. BE, supported by FR, suggested adding 'if the process concerns the data mentioned in Articles 8 and 9'.

⁵⁵ HU, supported by BG and SK, thought that a duty for the data controller to inform the data subject of a change of legal basis should be added here: 'Where personal data relating to the data subject are processed under this provision the controller shall inform the data subject according to Article 14 before the time of or within a reasonable period after the commencement of the first operation or set of operations performed upon the personal data for the purpose of further processing not compatible with the one for which the personal data have been collected.'

⁵⁶ Further to DE proposal.

Article 7

Conditions for consent

1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that unambiguous⁵⁷ consent was given by the data subject.
- 1a. Where article 9(2)(a) applies, the controller shall be able to demonstrate that explicit consent was given by the data subject.
2. If the data subject's consent is to be given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable (...) from the other matters.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (...).
4. (...)

⁵⁷ COM reservation related to the deletion of 'explicit' in the definition of consent.

Conditions applicable to child's consent in relation to information society services⁵⁸

1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child⁵⁹, the processing of personal data of a child below the age of **14 years**⁶⁰ shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child⁶¹. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

⁵⁸ CZ, DE, AT, SE, SI, PT and UK scrutiny reservation. CZ, SI and UK would prefer to see this Article deleted. UK thought children should not be singled out as the only category of vulnerable data subjects; NO proposes including a general provision stating that personal data relating to children cannot be processed in an irresponsible manner contrary to the child's best interest. Such a provision would give the supervisory authorities a possibility to intervene if for example adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child. DE, supported by NO, opined this article could have been integrated into Article 7. IE saw the merit of a provision on child protection and referred to the US where a robust child protection on-line exists. FR, supported by CZ, suggested to insert particular provision for children when the Articles of the data subjects' rights were discussed, *e.g.* Article 20 on profiling.

⁵⁹ Several delegations (HU, ES, FR, SE, SK, PT) asked why the scope of this provision was restricted to the offering of information society services or wanted clarification (DE) whether it was restricted to marketing geared towards children. The Commission clarified that this provision was also intended to cover the use of social networks, insofar as this was not governed by contract law. DE thought that this should be clarified. HU and FR thought the phrase 'in relation to the offering of information society services directly to a child' should be deleted.

⁶⁰ Several delegations queried the expediency of setting the age of consent at 13 years: BE, BG, CZ, DE, ES, FR, HU, HR, LU, LV, SK, PT, RO and SI. DE, ES, HR SI and RO proposed 14 years. COM indicated that this was based on an assessment of existing standards, in particular in the US relevant legislation (COPPA). FR and SK support setting the age of consent at 18 years (age of majority).

⁶¹ This term has been used in Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000. The Presidency suggests to add the definition from that Regulation (holder of parental responsibility" shall mean any person having parental responsibility over a child) to Article 4.

- 1a. Consent to the use of personal data of **children** for the purposes of **direct marketing [or creating personality or user profiles in the context of information society services]**⁶² shall be invalid⁶³.
2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child⁶⁴.
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 methods to obtain verifiable consent referred to in paragraph 1(...)⁶⁵.
4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)]⁶⁶.

Article 9

Processing of special categories of personal data⁶⁷

1. The processing of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life (...) shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies **and Article 6 is complied with**⁶⁸:

⁶² NL proposal.

⁶³ DE proposal. UK saw a lot of difficulties with paragraph 1a: concept of *minor; marketing* was out of the scope of the GDPR; impossibility to create personality/user profiles would have a negative impact on social services groups; not allowing user profiles would not be feasible. BG, CZ, DK and IE suggested to remove the paragraph.

⁶⁴ DE, supported by SE, queried whether a Member State could adopt/maintain more stringent contract law. SI thought the reference should be worded more broadly to 'civil law', thus encompassing also personality rights.

⁶⁵ ES, FR and SE scrutiny reservation.

⁶⁶ LU reservation. ES, FR, SE and UK suggested deleting paragraphs 3 and 4.

⁶⁷ COM, DK, SE, AT and NL scrutiny reservation. SK thought the inclusion of biometric data should be considered.

⁶⁸ Further to IE suggestion.

- (a) the data subject has given explicit consent to the processing of those personal data (...), except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or
- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject⁶⁹ in the field of employment and pensions law in so far as it is authorised by Union law or Member State law *or a collective agreement* pursuant to Member State law⁷⁰ providing for adequate safeguards⁷¹; or
- (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or
- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or
- (e) the processing relates to personal data which are manifestly made public⁷² by the data subject; or

⁶⁹ FI suggestion. COM scrutiny reservation.

⁷⁰ NL proposal.

⁷¹ DE queried whether this paragraph obliged Member States to adopt specific laws on data protection regarding labour law relations; COM assured that the paragraph merely referred to a possibility to do so.

⁷² DE, FR, SE and SI raised questions regarding the exact interpretation of the concept of manifestly made public (e.g. whether this also encompassed data implicitly made public and whether the test was an objective or a subjective one).

- (f) processing is necessary for the establishment, exercise or defence of legal claims⁷³; or
- (g) processing is necessary for (...) ⁷⁴ reasons of public interest, on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests; or
- (h) processing⁷⁵ is necessary for the purposes of preventive or occupational medicine⁷⁶, for the assessment of the working capacity of the employee⁷⁷, medical diagnosis, the provision of **health** care or treatment or the management of health-care systems and services (...) on the basis of Union law or Member State law⁷⁸ **or pursuant to contract to which the data subject is party** and subject to the conditions and safeguards referred to in paragraph 4⁷⁹;
- (ha) *processing of genetic data is carried out⁸⁰ for medical purposes⁸¹ and subject to the conditions and safeguards referred to in paragraph 4,⁸²*

⁷³ COM, IE and DE thought it should be clarified that also courts can process sensitive data.
⁷⁴ deletion of "for the performance of a task carried out for" at the suggestion of NL; AT and COM reservation on deletion of 'important'.

⁷⁵ HU suggested reinstating "of health data" here and in point (hb).

⁷⁶ AT and BE; BE pointed out this type of medicine practice is not (entirely) regulated by law under Belgian law and therefore the requirement of paragraph 4 is not met.

⁷⁷ AT and EE scrutiny reservation.

⁷⁸ COM, IE, PL scrutiny reservation.

⁷⁹ AT, DE and EE scrutiny reservation. DE and ES queried what happened in cases where obtaining consent was not possible (e.g. in case of contagious diseases; persons who were physically or mentally not able to provide consent); NL thought this should be further clarified in recital 42. BE queried what happened in the case of processing of health data by insurance companies. COM explained that this was covered by Article 9(2) (a), but SI was not convinced thereof.

⁸⁰ DE suggestion.

⁸¹ FR and IE reservation (IE remarked this did not cover the use these data for the purpose of establishing paternity); FR and SI wanted to deleted this point in its entirety. NL, RO and UK wanted to include also criminal purposes (*'the performance of a task carried out by competent authorities on the basis of Union or Member State law for the purpose of prevention, investigation, detection or prosecution of criminal offences'*), but the Presidency thinks this is covered by the draft Directive. Should this not be the case, this point would indeed need to be amended.

⁸² UK concerned this may restrict processing of data used for medical research.

- (hb) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject data;
- (i) processing is necessary for archiving purposes in the public interest or historical, statistical or scientific (...) purposes and subject to the conditions and safeguards referred to in Article 83 (...)⁸³.
- (j) [**processing is necessary for insurance and reinsurance, in particular the conclusion and the performance of insurance contracts, the processing of statutory claims, the evaluation of risks, the establishment of tariffs, compliance with legal obligations and the combating of insurance fraud**⁸⁴
and subject to the conditions and safeguards referred to in paragraph 4⁸⁵.]

3. (...) ⁸⁶

⁸³ The Presidency is of the opinion that when processing necessary for medical research, including studies conducted in the public interest in the area of public health, are covered by the concept of scientific purposes in Article 83 (and to the extent that would not be the case, should be covered by point (hb)). COM found that point (i) as regards health-related purposes was unclear and asked to explain further in a recital. COM wished that the substance of former Article 81 was maintained.

⁸⁴ Further to NL and DE suggestion, supported by FI and HR. This was however viewed critically by AT, BE, COM, EE, ES, FR, HU, IT, LU, MT, PT and SK. COM feared that it would go below the level of protection in 1995 Directive.

⁸⁵ Addition further to BE suggestion.

⁸⁶ COM reservation on the deletion of paragraph 3 on delegated acts.

4. *Personal data referred to in paragraph 1 may on the basis of Union or Member State law be processed for the purposes referred to in points (h) and (ha) of paragraph 2 when (...) those data are processed by **or under the responsibility**⁸⁷ of a (...) professional subject to the obligation of professional secrecy⁸⁸ under Union or Member State law or rules established by national competent bodies; by another person also subject to an (...) obligation of secrecy under Member State law or rules established by national competent bodies (...).*

[4a. In case a transfer of personal data referred to Article 44(1)(f) involves personal data concerning health such transfer can take place only subject to the condition that those data will be processed by a health professional subject to the obligation of professional secrecy under the law of the third State concerned or rules established by national competent bodies to the obligation of professional secrecy, or by another person also subject to an (...) obligation of secrecy under the law of the third State concerned or rules established by national competent bodies⁸⁹].

⁸⁷ Further to NL suggestion.

⁸⁸ See clarification of the term professional secrecy in recital 122. PL would have preferred to refer to legal obligations, but some of the may not be laid down in (statutory) law. RO on the contrary thought it sufficient to refer to 'rules established by national competent bodies in the field of professional secrecy'. IE reservation on this paragraph.

⁸⁹ COM, CZ, IE, NL, PT and FI reservation; EE, PL and UK scrutiny reservation. FR, supported by SK, proposed also to add an obligation of pseudonymisation. NL, FI and COM thought this should be regulated in Chapter V.

Article 9a

Processing of data relating to criminal convictions and offences⁹⁰

Alternative 1

Processing of data relating to criminal convictions and offences⁹¹ or related security measures **may only be based on points (c) and (e) of Article 6(1)**⁹² **and may only be carried out either under the control of official authority (...) or when the processing is authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of official authority**⁹³.

Alternative 2

Processing of data relating to criminal convictions and offences or related security measures **based on Article 6(1) may only be carried out either under the control of official authority (...) or when the processing is (...) authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of official authority**⁹⁴.

⁹⁰ SI reservation related to concerns on the possible impact on crime reporting by the media; CZ, BG, DE, ES, FI, HU, FR, NL, SK, SE, SI and UK scrutiny reservation. DE, EL and FR thought that these question related to the scope of the Directive and that it was necessary to know the delimitation of the scope of the two instruments to examine the Article. COM said that the Article was in line with Article 8(5) of the 1995 Directive.

⁹¹ BE thought that removing either *offences* or the reference to points (c) and (e) would make the Article acceptable.

⁹² NL believes reference to Article 6(1) and DK that the reference only to points (c) and (e) restrict the use of data.

⁹³ SI, SK and UK reservation on last sentence.

⁹⁴ UK reservation on last sentence.

Article 10

Processing not requiring identification

1. If the purposes for which a controller processes personal data do not require the identification of a data subject by the controller, the controller shall not be obliged to acquire (...) additional information nor to engage in additional processing in order to identify the data subject for the sole purpose of complying with (...) this Regulation⁹⁵.

2. Where, in such cases the controller is not in a position to identify the data subject, articles 15, 16, 17, 17a, 17b and 18 (...) do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification⁹⁶.

⁹⁵ AT, DE, FR, HU and UK scrutiny reservation.

⁹⁶ DK, NL, SE and SI scrutiny reservation; COM reservation. BE thought this paragraph could also be moved to a recital.