Council of the European Union

Brussels, 24 October 2014
(OR. en)

14705/14

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 146
JAI 802
MI 805
DRS 135
DAPIX 150
FREMP 178
COMIX 568
CODEC 2086

NOTE

From:	German delegation
To:	Working Party on Information Exchange and Data Protection
Subject:	Pseudonymisation

The German delegation welcomes the Presidency's efforts to emphasise the pseudonymisation and anonymisation of data as measures to reduce risks for data subjects. Anonymisation and pseudonymisation should not replace other protective measures, but instead reinforce them. Because processing pseudonymised data poses fewer risks for the rights and interests of data subjects, there is good reason to facilitate the processing of such data without removing them entirely from the scope of the Regulation.

The German delegation proposes taking the idea of pseudonymisation of data another step further, in order to encourage the use of pseudonymisation and make it more attractive to controllers while further improving the protection of data subjects. The German delegation therefore proposes the following additions to the text:

Art. 4 (3b) defines pseudonymisation as the application of measures making it impossible for the controller who processes the data to identify the data subject without disproportionate effort. Recital 23f explains that the "controller who processes the data" also refers to authorised persons within the same controller. This would allow companies to use data sets for statistical or research purposes ("Big Data") while minimising risks to data subjects. If the controller who processes the data re-identifies pseudonymised data using keys or other information so that individuals can be identified, such re-identification would be subject to the strict material conditions given in the new Art. 6 (5). This material threshold corresponds to the possibility to process data over the objection of the data subject given in the original Commission and European Parliament position, Art. 19. Thus by distinguishing between the rule (no identification) and the exception (possibility of identification), the idea of pseudonymisation measures may avoid the conflict between the necessary identification of the data subject and his or her desire not to be identified.

Recital 23 explains the conditions under which a person to whom the relevant data refer may be considered identifiable. This largely depends on how easy or difficult it is to acquire the information necessary for identification. Only those means need to be taken into account which can be used with a reasonable amount of time, expense and effort expended by the controller. It also notes that anonymous data do not come under the scope of the Regulation.

Changes are made to document 14270/14. Changes are made in **bold** and *italics*.

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 person.

23a) The application of pseudonymisation to 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) The general definition of pseudonymisation in Article 4 (3b) shall apply to all sectors that fall under the material scope of this Regulation. Numerous articles of this Regulation provide for a margin of manoeuvre for Member State law to define 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 specific and suitable technical implementation measures for pseudonymisation and additional requirements for encryption.

23c) 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 (Art. 6 (3a) (f)).

23d) (Re-)identification is the act of revealing individual data subjects in pseudonymised data sets. Individuals can be (re-)identified by cross-referencing pseudonymised data sets with a related set of data that includes identifiers or pseudonymisation keys or other data sources, using inference, deduction and/or correlation to identify individuals. The additional information for (re)-identification should be kept separately and should be subject to technical and organisational measures to ensure non-attribution. Under specific circumstances (re)-identification of the data subject should be allowed if the controller demonstrates compelling legitimate grounds which override the interests or fundamental rights and freedoms of the data subject. The controller shall consider all the determinants of risk and assess whether a threat to the data subject exists. In addition to stronger pseudonymisation techniques, controllers shall put in place stringent administrative and legal safeguards to minimize the risk of (re)-identification. Any unlawful (re)-identification constitutes an infringement or violation and should be subject to appropriate, proportionate and effective sanctions including compensation for damages suffered as a result of an infringement of data protection rules.

23e) ***This Regulation shall not prescribe particular safeguards, but shall provide for a broad range of measures to consider in a privacy impact assessment as appropriate for a particular data analysis. The broad approach to safeguards shall include the use of encryption, trusted third-party arrangements, use of pseudonymisation keys and arrangement for separation and security of decryption keys within the organisation of a controller or among several controllers, contractual restrictions on the disclosure of data, training of staff with access to the data, professional secrecy or other confidentiality obligations, personal background checks for those granted access to the data.***

23f) ***In order to create incentives for pseudonymisation, measures of pseudonymisation whilst allowing general analysis shall 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-data.***

24) ***Art. 7a gives data subjects the right to use aliases in information society services and serves two purposes: the effective exercise and enforcement of their right to freedom of expression within the framework of this Regulation and the ascertainment of the principles stipulated in Article 5 of this Regulation, namely data economy and use of pseudonymised data where applicable. The freedom to use blogs, forums and social networks and hold opinions is an expression of the rights conferred in Art. 11 of the Charter of Fundamental Rights of the European Union. The exercise of this right however shall not preclude necessary measures of criminal proceedings, especially measures to combat cyber-crime.***

Article 4

Definitions

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly (…), in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

[…]

(3b) "Pseudonymisation" means a processing of personal data by the controller in which all attributes revealing the identity of a natural person have been replaced with another attribute by the visible use of applications or measures, in a way that, without knowledge of the attribution system which is kept separately and subject to distinct technical and organizational measures, the information can no longer be attributed 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 manpower.

(3c) "Re-identification" is the identification of a data subject especially through data linkage techniques, such as cross-referencing of pseudonymised data sets with a related set of data, such as identifiers or pseudonymisation keys or other data sources, using inference, deduction and/or correlation.

Article 5

Principles relating to personal data processing

1. Personal data must be:

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

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

(c) adequate, relevant and not excessive in relation to the purpose for which they are processed;

(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 measures of pseudonymisation or anonymisation at the earliest possible stage***;

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

(f) (…)

2. Compliance with fair processing referred to in paragraph (1) (a) means

(a) …

(b) …

[Subject of another German Note coming soon]

(f) the use of privacy-enhancing technologies, such as anonymisation and pseudonymisation applied at the earliest possible stage, having regard to available technology and the cost of implementation, in order to minimise the risk for the rights and freedoms of the data subject.

Article 6

Lawfulness of processing

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

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

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

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

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

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

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a controller to which the data are disclosed 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. ***In assessing the interests it should be taken into account that the controller or personnel of the controller has taken effective measures of pseudonymisation of personal data in order to minimize the risk of the data subject. In such cases there is a refutable presumption that the subject's interests and fundamental rights and freedoms do not override the controller's interests.***

This subparagraph shall not apply to processing carried out by public authorities.

2. (…)

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

(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. Within the limits of this Regulation, the controller, processing operations and processing procedures, including measures to ensure lawful and fair processing, may be specified in this legal basis.

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, inter alia:

(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,;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards;

(f) whether measures of anonymisation or pseudonymisation have been applied to the data.

4. 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 (e) of paragraph 1.

5. Where personal data are pseudonymised, the re-identification of the data subject and further processing of these data shall only be allowed based on points (a), (b), (c), (d) or (e) of Article 6 (1), or if the controller demonstrates compelling legitimate grounds for the re-identification which override the interests or fundamental rights and freedoms of the data subject. The same applies to personal data which have been anonymized by the controller if they are attributable to a data subject again.

Article 7a

Right to use aliases in information society services

Data subjects shall have the right to use an alias, nickname or assumed name instead of their real name in information society services, having regard to the state of the art and the purpose of the service. The controller shall inform the data subject of this possibility.

SECTION 2

INFORMATION AND ACCESS TO DATA

Article 14 a

Information to be provided where the data have not been obtained from the data subject

[…]

4. Paragraphs 1 to 3 shall not apply where and insofar as:

(b) the provision of such information **(…)** proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of such purposes; in such cases the controller shall take appropriate measures to protect the data subject's legitimate interests, for example by ***pseudonymisation of personal data***; or

Article 15

Right of access for the data subject

[…]

5. Paragraphs 1 to 4 shall also apply to data that are processed under an alias in accordance with Article 7a. The request for information may be submitted under the alias.

[…]

Article 20

Profiling

[Pseudonymisation plays an important role in the regulation concerning "profiling". this topic has to be discussed with Article 20 again. Another German Note concerning „Profiling" is in preparation.]

[Furthermore the concept of pseudonymisation has to be reconsidered with Chapter IV.]