COUNCIL OF THE EUROPEAN UNION

Brussels, 20 January 2014

5332/1/14 REV 1

LIMITE

Interinstitutional File: 2012/0011 (COD)

DATAPROTECT 3
JAI 21
MI 34
DRS 5
DAPIX 3
FREMP 3
COMIX 27
CODEC 88

NOTE

from:	Presidency
to:	Working Group on Information Exchange and Data Protection (DAPIX)
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) - Pseudonymisation

Delegations will find attached the Presidency's proposals regarding pseudonymisation.

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

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.

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.

The processing of personal data to the extent strictly necessary for the purposes of preventing and monitoring 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.

Article 4

Definitions

For the purposes of this Regulation:

[...]

(3b) 'pseudonymisation' ~~'pseudonymous data'~~ **means the** processing of **personal data** ~~processed~~ **in such a way that the data can** ~~not~~ 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.**

Article 14 a

Information to be provided where the data have not been obtained from the data subject[1]

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

(b) the provision of such information **(…)**[2] proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of such purposes;[3] in such cases the controller shall take appropriate measures to protect the data subject's legitimate interests[4], for example by **pseudonymisation of personal** data[5]; or

1 DE, EE, ES, NL (§§1+2),AT, PT scrutiny reservation.
2 Deleted in view of the new articles 83a to 83c
3 COM scrutiny reservation.
4 Several delegations (DE, DK, FI, PL, SK, and LT) thought that in this Regulation (contrary to the 1995 Directive) the text should be specified so as to clarify both the concepts of 'appropriate measures' and of 'legitimate interests'. According to the Commission, this should be done through delegated acts under Article 15(7). DE warned that a dangerous situation might ensue if these delegated acts were not enacted in due time.
5 BE, FR and IT reservation on the mentioning of pseudonymous data.

Article 23

Data protection by design and by default[1]

1. Having regard to available technology and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing, the controller shall (…), implement (…) technical and organisational measures appropriate to the processing activity being carried on and its objectives, including **pseudonymisation of personal** data, in such a way that the processing will meet the requirements of this Regulation and (…) protect the rights of (…) data subjects.[2]

Article 30

Security of processing

1. Having regard to available technology and the costs of implementation and taking into account the nature, context**,** scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller and the processor[3] shall implement appropriate technical and organisational measures, including **pseudonymisation of personal** data to ensure a level of security appropriate to these risks.

---

1 DE scrutiny reservation; UK reservation: UK thought this should not be set out in the Regulation. FR scrutiny reservation: FR and LT sought clarification on the scope of the data protection by design and by default and on why the processor was not included. DE and MT thought that more emphasis should be put on pseudonymising and anonymising data. DE thought that, in view of Article 5(c), the principle of data economy and avoidance, as well as anonymisation and pseudonymisation should be listed as key options for implementation. It also thought data protection by design and by default should be more used in response to risky data processing operations. ES thought that the term 'non-excessive data processing' was preferable to 'data protection by design'. FR also queried the exact meaning of the terms used in the title.

2 NL stated this paragraph added little in terms of legal obligations compared to other articles in the draft regulation. It might be moved to a recital.

3 Several delegations thought that the controller should have the main responsibility (NO, NL, RO, UK).

Article 32

Communication of a personal data breach to the data subject[1]

3. The communication (…) to the data subject referred to in paragraph 1 shall not be required if**:**

   a. the controller (…)[2] has implemented appropriate technological protection measures and (…) those measures were applied to the data affected by the personal data breach, in particular those that[3] render the data unintelligible to any person who is not authorised to access it, such as encryption **(…)**[4] [5]; or

[1] AT scrutiny reservation. COM reservation: the consistency with the E-Privacy Directive regime should be safeguarded. NL thought there should be an exception for statistical data processing. FR thought that the possible application to public/private archives required further scrutiny.

[2] NL and FR criticised the subjective criterion of satisfying to the satisfaction of the DPA. More generally, NL opined that there was danger of the data protection authority would obtain company secrets from the data controller which the DPA might be obliged to disclose under access to document legislation.

[3] BE proposed 'have the purpose'.

[4] AT, FR, IT and PT reservation on reference to pseudonymised data. See however new recital 68a.

[5] MT and UK thought this exception should also be inserted to Article 31. There might nevertheless be cases where it still might be useful to inform the DPA.

Article 38

Codes of conduct [12]

1a. Associations and other bodies representing categories of controllers or processors[3] may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:

(bb) the **pseudonymisation of personal** data[4];

_____

1 AT, DK, FI, SK and PL scrutiny reservation. DE, FR and SI stated that this article should not apply to the public sector.

2 Several delegations thought more incentives should be made to apply to the use of codes of conduct: BE, DE, DK, LV, SE, SI, UK. Several delegations thought that hortatory language was being used in §1 (SI, PT), §1c (NL, SI, FR)

3 LU pleaded in favour of extending this to multinational companies established in various Member states.

4 FR scrutiny reservation.