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.*~~