COMP Article 30
17.10.2013

Article 30
Security of processing

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

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

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

3. The ***European Data Protection Board*** ~~***Commission***~~ shall be ***entrusted with the task*** ~~***empowered to adopt delegated acts in accordance with Article 86 for the purpose***~~ of ***issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b)*** ~~***further specifying the criteria and conditions***~~ for the technical and organizational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing

situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, ~~***unless paragraph 4 applies***~~.

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

Recitals

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, ~~***the Commission should promote***~~ technological neutrality, interoperability and innovation ***should be promoted***, and, where appropriate, ***cooperation with*** third countries ***should be encouraged***.