General Data Protection Regulation (EU) 2016/679 - References to 'security'*

Article 4: Definitions

(12) **'personal data breach' means a breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Recital 39: Principles relating to processing of personal data

...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 use of personal data and the equipment used for the processing…

Article 5: Principles relating to processing of personal data

(1) Personal data shall be: (f) processed in a manner that ensures **appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

(2) The controller shall be responsible for, and be able to **demonstrate compliance with, paragraph 1** ('accountability').

Article 30: Records of processing activities

(1) **Each controller** and, where applicable, the controller's representative, **shall maintain a record of processing activities** under its responsibility. **That record shall contain** all of the following information: (g) **where possible, a general description of the technical and organisational security measures referred to in Article 32(1).**

Recital 83: Security of processing

In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. **In assessing data security risk, consideration should be given to the risks that are presented by personal data processing**, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Article 32: Security of processing

(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, **the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk,** including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2) **In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing**, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

(3) Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

Recital 85: Notification obligation of breaches to the supervisory authority**

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, **the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons**. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Article 33: Notification of a personal data breach to the supervisory authority**

(1) In the case of a personal data breach, **the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.** Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

(2) The notification referred to in paragraph 1 shall at least: (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Recital 86: Notification of data subjects in case of data breaches**

The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

Article 34: Communication of a personal data breach to the data subject**

(1) **When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay**.

(3) The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

Recital 88: Format and procedures of the notification**

In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, **due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures**, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

Recital 75: Risks to the rights and freedoms of natural persons***

The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

Article 35: Data protection impact assessment

(1) **Where a type of processing** in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, **is likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, **prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data**.

(7) The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest 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 referred to in paragraph 1; (d) and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation** taking into account the rights and legitimate interests of data subjects and other persons concerned

Recital 49: Network and information security as a legitimate interest

The processing of personal data to the extent strictly necessary and proportionate 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 personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by 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

Article 40: Codes of conduct

(2) **Associations and other bodies representing categories of controllers or processors may prepare codes of conduct,** or amend or extend such codes, **for the purpose of specifying the application of this Regulation, such as with regard to**: (h) the measures and procedures referred to in Articles 24 and 25 and **the measures to ensure security of processing referred to in Article 32**; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

Article 45: Transfers on the basis of an adequacy decision

(2) **When assessing the adequacy of the level of protection**, the Commission shall, in particular, **take account of** the following elements: (a) the rule of law..as well as the **implementation of** such legislation, data protection rules, professional rules and **security measures**...

Article 47: Binding corporate rules

(2) **The binding corporate rules referred to in paragraph 1 shall specify at least:** (d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, **measures to ensure data security**, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules

* Direct extracts from GDPR text. Excludes references to national or public security. Sourced from this site: https://gdpr-info.eu/page/1/?s=security **Included by exception as key basis for the assessment of impact when considering personal data processing security risk and control adequacy.***Although breach notification Articles do not specifically mention the word security they are included in Chapter 2 Section 4: Security of Personal Data. Related recitals also included.