Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

CHAPTER IV

Controller and processor

Section 2

Security of personal data

Article 29

Security of processing

1 Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10.

2 In respect of automated processing, each Member State shall provide for the controller or processor, following an evaluation of the risks, to implement measures designed to:

a deny unauthorised persons access to processing equipment used for processing (‘equipment access control’);

b prevent the unauthorised reading, copying, modification or removal of data media (‘data media control’);

c prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (‘storage control’);

d prevent the use of automated processing systems by unauthorised persons using data communication equipment (‘user control’);

e ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation (‘data access control’);

f ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment (‘communication control’);

g ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input (‘input control’);

h prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (‘transport control’);

i ensure that installed systems may, in the case of interruption, be restored ('recovery');

j ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

Article 30

Notification of a personal data breach to the supervisory authority

1 Member States shall, in the case of a personal data breach, provide for the controller to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, 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 processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3 The notification referred to in paragraph 1 shall at least:

a describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c describe the likely consequences of the personal data breach;

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.

4 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5 Member States shall provide for the controller to document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

6 Member States shall, where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, provide for the information referred to in paragraph 3 to be communicated to the controller of that Member State without undue delay.

Article 31

Communication of a personal data breach to the data subject

1 Member States shall, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, provide for the controller to communicate the personal data breach to the data subject without undue delay.

2 The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and measures referred to in points (b), (c) and (d) of Article 30(3).

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 technological 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;

c it would involve a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

4 If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph 3 are met.

5 The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 13(3).