

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');

Status: EU Directives are being published on this site to aid cross referencing from UK legislation. After IP completion day (31 December 2020 11pm) no further amendments will be applied to this version.

- 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').