Personal data protection: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data

2012/0010(COD) - 27/04/2016 - Final act

PURPOSE: to ensure effective judicial cooperation in criminal matters and police cooperation and to facilitate the exchange of personal data between competent authorities of Member States, whilst ensuring a consistent and high level of protection of the personal data of natural persons (reform of data protection).

LEGISLATIVE ACT: Directive (EU) 2016/680 of the European Parliament and of the Council 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.

CONTENT: the new Directive aims to **protect personal data that is processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,** including the safeguarding against and the prevention of threats to public security. It responds to the need to ensure a high and systematic level of data protection for natural persons whilst at the same time facilitating the exchange of these data between the law enforcement services of different Member States.

The reform of data protection also includes a new General Data Protection Regulation (intended to replace 95/46/EC).

The main elements of the Directive are as follows:

Scope: the Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. It applies to **cross-border processing** of personal data as well as processing of this data at national level.

The directive applies **not only to competent public authorities but also to any other body or entity** entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Principles relating to processing of personal data: Member States shall provide for personal data to be:

- processed lawfully and fairly;
- collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are processed;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;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.

Processing purposes: the Directive provides that processing by the same or another controller for any of the purposes set out in the directive other than that for which the personal data are collected shall be **permitted in so far as the controller is authorised to process such personal data for such a purpose** in accordance with Union or Member State law, and that processing is necessary and proportionate to that other purpose.

Time-limits for storage and review: Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.

Categories of data subject: Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects.

Lawfulness of processing: processing shall be lawful only if it is **necessary** to carry out a particular task by a competent authority, for the purposes set out in the Directive, in accordance with Union or Member State law.

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be **allowed only where strictly necessary**, subject to appropriate safeguards for the rights and freedoms of the data subject.

A decision based solely on **automated processing, including profiling**, which produces an adverse legal effect concerning the data subject or significantly affects him or her, is prohibited unless authorised by Union or Member State law and unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Rights of the data subject: the new rules include:

- the right of the subject to be **informed**, in clear and simple terms, that the data concerning him are being processed;
- the right of the data subject to be informed about the identity and the contact details of the controller and the purposes of the processing for which the personal data are intended;
- the right of **access** by the data subject to personal data and the grounds for being refused access to that information;
- the right to **rectification or erasure** of personal data concerning the data subject or restriction on processing of such data.

Responsibility of the controller or processor: the Regulation establishes the legal framework on the responsibility and liability for any processing of personal data carried out by a controller or, on the controller's behalf, by a processor. The controller is obliged to implement appropriate technical and organisational measures and be able to demonstrate the compliance of its processing operations with the Regulation.

The new Directive provides that the controller shall designate **a data protection officer** to assist the supervisory authority on issues relating to processing.

Impact assessment: the impact assessment constitutes a tool to ensure that the provisions are observed. The controller should carry out a data protection impact assessment where the processing operations, in particular using new technologies, are likely to result in a high risk to the rights and freedoms of data subjects.

The controller or processor should consult the supervisory authority prior to processing which will form part of a new filing system to be created where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Transfers of personal data outside the EU: the new rules also cover the transfer of personal data to a third country or to an international organisation. This transfer may only take place where the **Commission decides** that the third country or an international organisation ensures an adequate level of protection. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the rule of law, respect for human rights and fundamental freedoms, and the existence and effective functioning of one or more independent supervisory authorities in the third country.

Where personal data are transmitted from another Member State, that Member State must have given its prior authorisation to the transfer. Transfers from another Member State without prior authorisation will be permitted only when the transfer is necessary to prevent an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time.

Supervisory authority: in order to ensure compliance with the rules of the Directive, supervisory authorities will carry out monitoring of the application of the Directive.

Liability and sanctions: the new Directive also gives data subjects the right to effective judicial redress against a prejudicial decision by a supervisory authority and the right to obtain compensation in case of damage following a breach of the Regulation.

ENTRY INTO FORCE: 5.5.2016.

TRANSPOSITION: by 6.5.2018. A Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.