Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 27/04/2016 - Final act

PURPOSE: to modernise the existing rules on data protection in order to ensure a high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union (reform of data protection).

LEGISLATIVE ACT: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

CONTENT: the new Regulation **establishes rules on the protection of natural persons with regard to the processing of personal data and on the free movement of such data**. It protects the fundamental rights and freedoms of natural persons, and particularly their right to protection of their personal data. The reform of data protection also includes a Directive on protection of data processed for the purpose of law enforcement (intended to replace the 2008 Framework Decision on data protection.)

The main points are as follows:

Scope: the Regulation 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 the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, **regardless of whether the processing takes place in the Union or not**.

Principles relating to processing of personal data: personal data shall be:

- **processed lawfully, fairly and in a transparent manner** in relation to the data subject;
- **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- **kept** in a form permitting identification of the person concerned for a period that does not exceed what is necessary for the purposes of processing;
- 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.

Lawfulness of processing: processing shall be lawful only if:

- the data subject has clearly and explicitly given consent to the processing;

- **processing is necessary** for: (i) the performance of a contract; (ii) compliance with a legal obligation; (iii) protecting the vital interests of the data subject or of another natural person; (iv) the performance of a task carried out in the public interest; (v) the purposes of the legitimate interests pursued by the controller or by a third party.

A specific protective regime is provided for consent by **children** in relation to the offering of information society services: if a **child below the age of 16 years** wishes to use online services, the service provider must verify that those with parental responsibility over the child have given their consent. Member States may lower this age limit, but it may not be below 13 years.

In principle, 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 prohibited. The data may, however, be processed under certain conditions set out in the Regulation.

Rights of the data subject: the Regulation sets out stronger rights in respect of data protection and strengthens the accountability of controllers. The rights of the data subject include:

- **the right to information:** this information must be concise, transparent, intelligible and easily accessible form, in particular for any information addressed specifically to a child. Natural persons must be informed about the policy in force with respect to data protection, in clear and simple terms; this may also be done through standardised icons;

- **the right of access to personal data**, i.e. the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where such personal data are being processed, access to the information concerning, e.g. the purposes of the processing for which the personal data are intended, data categories, the recipients of the personal data, and where possible, the period for which the personal data will be stored;

- **the right of rectification** of incorrect data;

- **the right to erasure** to erasure of personal data, including the "**right to be forgotten**";

- **the right to restriction of processing**;

- **the right to data portability**, facilitating the transfer of personal data from one service provider, such as a social network, to another;

- **the right to object** and the right not be the subject of automated decision-making, including **profiling**. Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing.

These rights may be restricted where such restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to **safeguard national security, defence or public security**.

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.

Data security: in order to maintain security and to prevent processing in infringement of the 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.

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 controller should also 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.

Data protection officer: the controller and the processor shall designate a data protection officer in any case where a public authority or body carries out the processing. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under the Regulation.

Transfers of personal data outside the EU: as a general principle any transfer of personal data to a third country or to an international organisation may only take place if the controller and processor **comply with the rules** under the Regulation.

The Commission will decide, through implementing acts, that the third country or an international organisation ensures an adequate level of protection. The implementing act shall provide for a mechanism for a periodic review, at least every four years.

Supervision: to increase legal certainty and reduce administrative burden, in cross-border cases involving several national supervisory authorities, a **consistency mechanism is established**. The mechanism allows an enterprise active in several Member States to deal only with the data protection authority in the Member State in which it has its main establishment. The mechanism also provides for a single decision applicable to the whole EU in case of disputes.

Redress, responsibility and penalties: the Regulation sets out a detailed set of rules to allow persons to **claim judicial redress or compensation in case of damage** following a breach of the Regulation.

The Regulation provides that non-compliance with an order by the supervisory authority shall be subject to administrative fines up to **EUR 20 000 000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher.

ENTRY INTO FORCE: 24.5.2016.

APPLICATION: from 25.5.2018.

DELEGATED ACTS: the Commission may adopt delegated acts, particularly in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. The power to adopt such acts is conferred on the Commission for **an indeterminate period from 24 May 2016**. The European Parliament or the Council may raise objections to a delegated act within **three months** of the date of notification (this may be extended by three months.) If Parliament or Council raise objections, the delegated act will not come into force.