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

2012/0011(COD) - 12/03/2014 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 621 votes to 10 with 22 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Parliaments position in first reading following the ordinary legislative procedure amended the Commission proposal as follows:

Territorial Scope: Parliament stated that the Regulation applied whether the processing takes place in the Union or not. It applied to the processing of personal data of data subjects in the Union by a controller or processor not established in the Union, where the processing activities are related to linked.

Principles relating to personal data processing: these are: (i) lawfulness, fairness and transparency; (ii) purpose limitation; (iii) data minimization; (iv) accuracy; (v) storage minimization; (vi) integrity, meaning protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; (vii) accountability.

Conditions of consent: the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be likely stored for each purpose, if the data are to be transferred to third parties or third countries.

Where processing is based on the data subjects consent, Parliament confirmed that the controller should have the burden of proving that the data subject has given the consent to the processing operation.

Members added that:

- provisions on the data subjects consent which are partly in violation of this Regulation are fully void;
- it should be as easy to withdraw consent as to give it. The data subject shall be informed by the controller if withdrawal of consent may result in the termination of the services provided or of the relationship with the controller.
- consent shall be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected.

Information provided to children, parents and legal guardians in order to express consent, including about the controllers collection and use of personal data, should be given in a clear language appropriate to the intended audience.

The following is prohibited: the processing of personal data, revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, and the processing of genetic or biometric data or data concerning health or sex life, administrative sanctions, judgments, criminal or suspected offences, convictions or related security measures.

General principles for data subject rights: Parliament proposed to strengthen, clarify, guarantee and where appropriate, codify these rights, which should be clear and unambiguous, and include:

- the provision of clear and easily understandable information regarding the processing of his or her personal data,
- the right of access, rectification and erasure of their data,
- the right to obtain data,
- the right to object to profiling, being any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural persons performance at work, economic situation, location, health, personal preferences, reliability or behaviour;
- the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as
- the right to compensation and damages resulting from an unlawful processing operation.

Such rights shall in general be exercised free of charge. The data controller shall respond to requests from the data subject within a reasonable period of time.

Standardised information policies: Parliament introduced a new Article stating that where personal data relating to a data subject are collected, the controller shall provide the data subject in an easily visible and clearly legible way and in a language easily understood - with certain particulars listed in the text before providing information required by the Regulation.

Such particulars include: (i) whether personal data are collected beyond the minimum necessary for each specific purpose of the processing, and (ii) whether personal data are processed for purposes other than the purposes for which they were collected; (iii) whether personal data are disseminated to commercial third parties or sold or rented out; (iv) whether personal data are retained in encrypted form.

Right to erasure: Members reinforced this right by allowing the data subject to obtain from third parties the erasure of any links to, or copy or replication of, that data where one of the following grounds applies:

- a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;
- the data has been unlawfully processed.

Where the controller has made the personal data public without a justification, it shall take all reasonable steps to have the data erased, including by third parties. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.

Profiling: Parliament clarified that all persons have the right to object to profiling. The person concerned shall be informed about the right to

object to profiling in a highly visible manner.

Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling.

Parliament added that profiling which leads to measures producing legal effects concerning the data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment.

Security of processing: such a security policy shall include the ability: (i) to ensure that the integrity of the personal data is validated; (ii) to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; (iii) to restore the availability and access to data in a timely manner in the event of a physical or technical incident.

Transfers or disclosures not authorised by Union law: a new Article provides that no judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognised or be enforceable in any manner (without prejudice to international agreements).

Lead authority: where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, Parliament proposed that the supervisory authority of the main establishment of the controller or processor shall act as the lead authority responsible for the supervision of the processing activities of the controller or the processor in all Member States.

Administrative sanctions: to anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:

- a warning in writing in cases of first and non-intentional non-compliance;
- regular periodic data protection audits;
- a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is higher.

If the controller or the processor is in possession of a valid "European Data Protection Seal", a fine shall only be imposed in cases of intentional or negligent incompliance.