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

2012/0011(COD) - 22/11/2013 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the report by Jan Philipp Albrecht (Greens/EFA) 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).

The committee recommended that the Parliament's position adopted in first reading following the ordinary legislative procedure should amend the Commission proposal. The key amendments are as follows:

Territorial Scope: the report provides that the Regulation 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, **whether the processing takes place in the Union or not**. It applies to a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union.

Consent to processing: where processing is based on consent, the report confirms the controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. It adds that:

- provisions on the data subject's consent which are partly in violation of the Regulation are fully void;

- it shall 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. The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service.

Right to erasure: the amendment in the report **reinforces the right to erasure of data** by allowing the data subject the right to obtain from third parties (to whom the data have been passed) the erasure of any links to, or copy or replication of that data. It also adds that the data subject has the right to erasure where:

- 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.

The controller and, where applicable, the third party shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary under certain specified grounds.

Notification requirement in the event of rectification and erasure: the controller shall communicate any rectification or erasure to each recipient to whom the data have been transferred, unless this proves impossible or involves a disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests this.

Standardised information policies: a new Article states that where personal data relating to a data subject are collected, the controller shall provide the data subject with certain particulars listed in the text before providing information required by the Regulation. Such particulars include whether personal data are collected beyond the minimum necessary for each specific purpose of the processing, and whether personal data are disseminated to commercial third parties.

The data controller would also be required to inform the person about various aspects of the data processing, such as the period of storage, the recipients of the personal data and the possible existence of profiling, as well as the data subject's rights of access, rectification and erasure of the data and right to lodge a complaint with a data protection authority.

Data portability: the committee deleted the Commission's provisions on data portability. The report provides that where personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data **in an electronic and interoperable format** which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the **data shall be transferred directly from controller to controller at the request of the data subject.**

Profiling: the report strengthens the **data subject's right to object to profiling**. The data subject 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.

The committee adds 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.

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). Where such a request is made of a controller, the latter must obtain prior authorisation for the transfer or disclosure by the supervisory authority. The data subjects must be informed.

A recital in the text adds that in cases where controllers or processors are confronted with **conflicting compliance requirements** between the jurisdiction of the Union on the one hand, and that of a third country on the other, the Commission should ensure that Union law takes precedence at all times. The Commission should provide guidance and assistance to the controller and processor, and it should seek to resolve the jurisdictional conflict with the third country in question.

Lead Authority: the report provides that where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one

Member State, **one single supervisory authority should act as the single contact point and the lead authority responsible**. The lead authority, providing a one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment or its representative. **The European Data Protection Board may designate the lead authority through the consistency mechanism in certain cases** on the request of a competent authority. The lead authority must consult other competent supervisory authorities in an endeavour to reach a consensus. However, it shall be the sole authority empowered to decide on measures intended to produce legal effects as regards the processing activities of the controller or processor for which it is responsible.

Data Protection Officers: the controller and the processor shall designate a data protection officer inter alia, where the processing is carried out by a legal person and relates to more than 5000 data subjects in any consecutive 12-month period.

Data protection officers shall be **bound by secrecy concerning the identity of data subjects** and concerning circumstances enabling data subjects to be identified, unless they are released from that obligation by the data subject. The committee changed the criterion from the number of employees a company has (the Commission suggested at least 250), to the number of data subjects. DPOs should be appointed for **at least four years** in the case of employees and two in that of external contractors. The Commission proposed two years in both cases.

Data protection officers should be in a position to perform their duties and tasks independently and **enjoy special protection against dismissal**. Final responsibility should stay with the management of an organisation. The data protection officer should be consulted prior to the design, procurement, development and setting-up of systems for the automated processing of personal data, in order to ensure the principles of privacy by design and privacy by default.

Administrative sanctions: additional provisions state that 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 (the Commission proposed up to EUR1 million or 2% of annual worldwide turnover). 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.

The administrative sanction shall take into account certain prescribed factors including the intentional or negligent character of the infringement, the degree of co-operation with the supervisory authority, in order to remedy the infringement and the level of damage, including non-pecuniary damage, suffered by the data subjects.