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) - 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 Dimitrios Droutsas (S&D, EL) on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

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:

Minimum standards in the Directive: EU countries may set higher standards than those enshrined in the Directive.

Principles relating to personal data processing: personal data must be processed lawfully, fairly and in a transparent and verifiable manner in relation to the data subject. Such data must be adequate, relevant, and **limited to the minimum necessary** in relation to the purposes for which they are processed. They shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data.

The controller must implement technical and organisational measures to prevent accidental loss, destruction or damage.

Access to data initially processed for other purposes: the committee added in a new Article stating that competent authorities may only have access to personal data initially processed for purposes other than those referred to in the text if they are specifically authorised by Union or Member State law which must meet the requirements set out.

Access is allowed only by **duly authorised staff** of the competent authorities in the performance of their tasks.

Time limits of storage and review: personal data processed **shall be deleted** by the competent authorities where they are no longer necessary for the purposes for which they were processed. Competent authorities must put mechanisms in place to **ensure that time-limits are established for the erasure of personal data** and for a periodic review of the need for the storage of the data, **including fixing storage periods for the different categories of personal data.** Procedural measures shall be established to ensure that those time limits or the periodic review intervals are observed.

Different categories of data subjects: the draft directive sets out provisions permitting processing of the personal data of the different categories of data subjects. Personal data of other data subjects than those

referred to may only be processed under strict conditions only for as long as necessary for the investigation or for targeted, preventive purposes.

Different degrees of accuracy and reliability of personal data: personal data based on facts must be distinguished from personal data based on personal assessments, in accordance with their degree of accuracy and reliability. The committee states that personal data that are inaccurate, incomplete or no longer up to date must not transmitted or made available. To this end, the **competent authorities shall assess the quality of personal data** before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, up-to-dateness and reliability. Personal data shall not be transmitted without request from a competent authority, in particular data originally held by private parties.

Members add that if it emerges that incorrect data have been transmitted or data have been transmitted unlawfully, the **recipient must be notified without delay** and is obliged to rectify the data or to erase them.

Lawfulness of processing: Member State law regulating the processing of personal data within the scope of this Directive shall contain explicit and detailed provisions specifying at least: (i) the objectives of the processing; (ii) the personal data to be processed; (iii) the specific purposes and means of processing; (iv) the appointment of the controller, or of the specific criteria for the appointment of the controller; (v) he categories of duly authorised staff of the competent authorities for the processing of personal data; (vi) the procedure to be followed for the processing; (vii) the use that may be made of the personal data obtained; (viii) limitations on the scope of any discretion conferred on the competent authorities in relation to the processing activities.

Profiling: the committee amendments strengthen safeguards against extensive profiling. Profiling remains permissible only under strict conditions. Automated processing of personal data intended to single out a data subject without an initial suspicion that the data subject might have committed or will be committing a criminal offence shall only be lawful to the extent that it is **strictly necessary for the investigation of a serious criminal offence** or the prevention of a clear and imminent danger, established on factual indications, to public security, the existence of the State, or the life of persons.

Data subjects are entitled to information about the logic used in the profiling and the **right to obtain human assessment**. Profiling that, whether intentionally or otherwise, has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, gender or sexual orientation, or that, whether intentionally or otherwise, results in measures which have such effect, shall be prohibited in all cases.

General principles for the rights of the data subject: such rights must include, inter alia, 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 his or her data**, the right to obtain data, 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.

Processing of genetic data for the purpose of a criminal investigation or a judicial procedure: the committee added provisions stating that genetic data may only be used to establish a genetic link within the framework of adducing evidence, preventing a threat to public security or preventing the commission of a specific criminal offence. They may **not be used to determine other characteristics** which may be linked genetically.

Such data may only be retained as long as necessary for the purposes for which data are processed and where the individual concerned has been convicted of serious offences against the life, integrity or security of persons, subject to **strict storage periods to be determined by Member State law.**

Data transferred to third countries: data transferred to competent public authorities in third countries should not be further processed for purposes other than the one they were transferred for. Further onward transfers from competent authorities in third countries or international organisations to which personal data have been transferred should **only be allowed if the onward transfer is necessary for the same specific purpose as the original transfer** and the **second recipient is also a competent public authority** . Further onward transfers should not be allowed for general law-enforcement purposes.

Derogations to these rules are set out in the report.

Powers: the report expands on the powers of supervisory authorities, which now include: (i) warning or admonishing the controller or the processor; (ii) ordering the rectification, erasure or destruction of all data when they have been processed in breach of the provisions; (iii) imposing a temporary or definitive ban on processing; (iv) informing national parliaments, the government or other public institutions as well as the public on the matter.

The report also **expands the supervisory authority's investigative power** to obtain from the controller or the processor certain information laid out in the text.

Each supervisory authority shall have the power to **impose penalties in respect of administrative offences.**

Data protection officer: he or she shall be appointed for a period of at least **four years** and may be reappointed for further terms. The data protection officer may only be dismissed from that function, if he or she no longer fulfils the conditions required for the performance of his or her duties.

Reporting of violations: Members stipulate that supervisory authorities must take into account guidance issued by the European Data Protection Board and, together with competent authorities, put in place effective mechanisms to encourage **confidential reporting of breaches** of the Directive.

Joint operations: where these take place, in cases where data subjects in other Member States are likely to be affected by processing operations, the competent supervisory authority may be invited to participate in the joint operations. It may invite the supervisory authority of each of those Member States to take part in the respective operation and in cases where it is invited, respond to the request of a supervisory authority to participate in the operations without delay.

Transmission of personal data to other parties: a new Chapter VIIIa states that the controller must not transmit or instruct the processor to transmit personal data to a natural or legal person not subject to the provisions adopted pursuant to the Directive, unless the prescribed conditions are met. These include the condition that the recipient is established in a Member State of the EU, and no legitimate specific interests of the data subject prevent transmission.