

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) - 12/03/2014 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 371 votes to 276 with 30 abstentions, a legislative resolution 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.

Parliament's position in first reading following the ordinary legislative procedure amended the Commission proposal as follows:

Minimum standards in the Directive: the Directive should protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of their personal data and privacy. It should not preclude Member States from providing higher safeguards than those it established.

Principles: personal data must be: (i) processed lawfully, fairly and in a transparent and verifiable manner in relation to the data subject; (ii) only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data; (iii) processed in a way that effectively allows the data subject to exercise his or her rights; (iv) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage; (v) processed by only those duly authorised staff of the competent authorities who need them for the performance of their tasks.

Personal data held by private parties or other public authorities shall only be accessed to investigate or prosecute criminal offences in accordance with necessity and proportionality requirements to be defined by Union law by each Member State in its national law.

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.

Different categories of data subjects: competent authorities may process personal data of different categories of data subjects. Personal data of other data subjects may only be processed under certain conditions, for example, when such processing is indispensable for targeted, preventive purposes or the investigation or prosecution of a specific criminal offence.

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. Personal data that are inaccurate, incomplete or no longer up to date must not be transmitted or made available. They shall not be transmitted without request from a competent authority, in particular data originally held by private parties.

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: the processing of personal data is lawful only if and to the extent that processing is based on Union or Member State law. Parliament stated that national 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; (v) the 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: Members added a definition of profiling and strengthen safeguards for persons concerned. Automated processing of personal data intended to single out a data subject without an initial suspicion that the data subject might have committed 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. Such processing should in no circumstances contain, generate, or discriminate based on special categories of data regarding race or ethnic origin, political opinions, religion or beliefs, trade union membership, gender or sexual orientation.

General principles for the rights of the data subject: the directive should aim to strengthen, ensure, clarify and if necessary, codify these rights. Such rights must include, inter alia: (i) 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, (ii) the right to obtain data, (iii) the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as (iv) 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: Parliament introduced new 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. 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: Parliament considered that the Commission proposal did not contain the safeguards necessary to protect the rights of persons whose data had been transferred. The amended text provided that where the Commission decides that a third country, or a territory within that third country, or an international organisation does not ensure an adequate level of protection, a controller or processor may not transfer personal data to a third country, or an international organisation **unless the controller or processor has adduced appropriate safeguards** with respect to the protection of personal data in a legally binding instrument.

These transfers must be **authorised by the supervisory authority prior to the transfer.**

Powers: Parliament strengthened the powers of supervisory authorities. The latter must have the same duties and effective powers in each Member State, including effective powers of investigation, power to access all personal data and all information necessary for the performance of each supervisory function, power to access any of the premises of the data controller or the processor including data processing requirements.

Supervisory authorities 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.

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

Transmission of personal data to other parties: Parliament introduced a new Chapter which provided that the controller must not transmit personal data to a natural or legal person not subject to the provisions adopted pursuant to the Directive, such as: (i) the transmission complies with Union or national law; (ii) the recipient is established in a Member State of the European Union; (iii) no legitimate specific interests of the data subject prevent transmission.