European Parliament

Data protection reform package: Final steps

A package to reform the EU legal framework on data protection (DP) was presented by the European Commission in January 2012. Aimed at strengthening citizens' rights uniformly while reducing burdens for companies and public authorities, the package takes a comprehensive approach, including a general regulation and a directive concerning data protection for police and law enforcement purposes. Following negotiations towards a second-reading agreement, compromises on both texts have been reached, and votes in plenary, scheduled for the April I session, are now required to confirm them.

Context

Personal data are increasingly collected and processed automatically for different purposes, ranging from commercial aims (e.g. personalised advertisements and services) to police activities (e.g. investigation and prosecution of crimes). Besides the benefits for society and individuals, data processing raises serious concerns about the potential impacts on individual dignity, rights and freedoms, including the right to privacy and non-discrimination. In order to allow people to make, as much as possible, their own decisions regarding the use of their data and to guarantee safeguards against potential abuses of data handling, clear and strict rules, to be applied consistently in the context of all EU policies, are necessary. The development of digital technologies and the emergence of a data-driven society – in which almost every daily activity requires the flow and combination of personal information – made it urgent to reform the current EU data-protection regime, dating back to 1995. The right to data protection enshrined in the EU Charter of Fundamental Rights also makes this reform necessary. Moreover, revelations on mass-surveillance programmes involving both companies and public authorities required a firm response from the EU institutions, with a view to restoring trust in the use of innovative technologies and practices.

General Data Protection Regulation (GDPR)

The Commission presented, back in 2012, a proposal for a general regulation (Rapporteur: Jan Philipp Albrecht, Greens/EFA, Germany), which would repeal Directive 95/46/EC. The Council favoured a law with reduced administrative burdens for companies; this approach was accepted by the Commission and the Parliament only on the condition of not watering down central principles of the 1995 Directive (e.g. informed consent, transparency, and necessity), and if balanced by strong provisions on individual rights and sound sanction mechanisms.

Intended as a wide-ranging and far-sighted reform to improve and harmonise data protection in the digital age, the long-awaited regulation would update most of the current rules and introduce new ones. According to Opinion 3/2015 of the European Data Protection Supervisor (EDPS), established principles of data protection should be maintained and applied in more dynamic, innovative, and therefore more effective, ways. The GDPR promises to improve both the internal market dimension and protection of citizens and consumers, by fostering individuals' trust in the Digital Single Market and by establishing legal certainty and consistency to make industrial investment in the EU more attractive. Once it enters into force, the regulation will be directly applicable in the Member States within two years, although many detailed provisions need to be set out at a later stage by Commission delegated and implementing acts.

What will change

Among other things, the regulation would enhance the level of data protection for individuals, and increase business opportunities by: reinforced consent requirement (to be explicit); increased transparency (better and clearer information); easier access to one's own data; a 'right to be forgotten' (if there are no legitimate grounds for retaining them, the data may be deleted); parental consent requirement for youngsters below 16 years to use online services (that may be lowered to 13 years by Member States); right to object to

Author: Shara Monteleone, **Members' Research Service**
PE 580.908

profiling; a right to data portability, allowing the transmission of personal data from one service provider (e.g. a social network) to another, while also enhancing competition among service providers; a single set of rules across the EU and wider scope of application of those rules (the regulation will also apply to non-EU companies that offer goods or services in the EU or monitor the online behaviour of citizens); data breaches notification (due by companies to supervisory authorities); one-stop shop (to allow a company operating in several Member States to deal with a single data protection authority, DPA); and the creation of a European Data Protection Board. Companies' requirements, in certain circumstances, include designation of a DP officer and a DP Impact Assessment. Technology developers will have to comply with the DP by Design and by Default (i.e. 'to embody' data protection requirements into a product or service as early as possible). Moreover, DPAs will be equipped with more powers and resources to apply meaningful remedies (e.g. effective fines). While the accountability principle would be reinforced, unnecessary administrative burdens would be removed. Although the renewed high European data protection standards may represent worrying challenges for some companies, they are also being promoted as an advantage for EU-based companies enabling them to compete better on a global level and contribute to the success of the economy.

Parliament's position at first reading was adopted with a resolution of 12 March 2014, after the Civil Liberties, Justice and Home Affairs (LIBE) Committee agreed in October 2013 on a heavily amended text (Albrecht report). On 15 June 2015 the Council reached a general approach, leading to trilogue negotiations. Council endorsed the agreement reached on 15 December 2015, and on 8 April 2016 it adopted its position at first reading. At a meeting on 12 April, the LIBE Committee adopted its recommendations for second reading by Parliament, due to take place during the April I plenary session the same week. Adoption by the Parliament of the Council's position, without amendment, will complete the legislative procedure.

Directive on data processing for law enforcement purposes

Along with the GDPR, the Commission proposed a directive on protecting data used for police and criminal justice purposes (Rapporteur: Marju Lauristin, S&D, Estonia). It aims to ensure that, in accordance with the EU Charter, law enforcement authorities protect personal data processed for prevention, investigation, detection or prosecution of criminal offences, including the prevention of threats to public security. The objective is to ensure a consistent and high level of data protection and other fundamental rights of individuals (whether they are a victim, witness, suspect or criminal) while enabling effective cooperation among law enforcement authorities and facilitating the exchange of personal data between Member States.

What will change

Data protection in the field of police and criminal justice (former Pillar III) was covered up to now by Council Framework Decision 2008/977/JHA, limited to the processing of data transmitted between Member States, and thus not including domestic data. The proposed directive would repeal that and needs to be transposed into national law in a harmonised way. It would contribute to building an Area of Freedom, Security and Justice with a high level of data protection. In particular, processing of data for law enforcement must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for individuals. Supervision should be ensured by independent national DP authorities, and effective judicial remedies must be provided. Parliament insisted on the mandatory presence of a Data Protection Officer within the competent authority to monitor all data transfers, as well as on an impact assessment to be carried out in cases when data processing entails high risk for a person's rights and freedoms. Obligations as regards DP by Design and by Default (e.g. pseudonymisation and data minimisation) should also be imposed. Notification of a data breach to the supervisory authority is also foreseen. In its Opinion 3/2015, the Article 29 Working Party (WP29) insisted on the importance of ensuring the necessary consistency between both texts of the package, also in light of the recent CJEU judgments in *Digital Rights Ireland* and *Schrems*.

Parliament's position at first reading was adopted with a resolution of 12 March 2014, after the LIBE Committee agreed in October 2013 on the Droutsas Report. On 9 October 2015 the Council reached a general approach on the proposed directive. A compromise in trilogue negotiations was reached on 15 December 2015, and on 8 April 2016 the Council adopted its position at first reading. At its meeting on 12 April, the LIBE Committee adopted its recommendation for second reading by Parliament, due to take place during the April I plenary session. Adoption by the Parliament, of the Council's position without amendment, will complete the legislative procedure.

The DP package is to be voted together with the PNR directive during the April plenary.