Council of the EU

PRESS
EN

PRESS RELEASE
951/15
18/12/2015

EU data protection reform: Council confirms agreement with the European Parliament

On 18 December 2015, the Permanent Representatives Committee (Coreper) confirmed the compromise texts agreed with the European Parliament on data protection reform. The agreement was reached between the Council, Parliament and Commission on the 15 December. This agreement is in line with the request from the European Council for negotiations on data protection reform to be concluded by the end of 2015.

Félix BRAZ, Luxembourg Minister of Justice and President of the Council said: "It is a fundamental agreement with important consequences. This reform not only strengthens the rights of citizens, but also adapts the rules to the digital age for companies, whilst reducing the administrative burden. These are ambitious and forward-looking texts. We can have full confidence in the result."

Data protection reform is a legislative package proposed by the Commission in 2012 to update and modernise the data protection rules. It concerns two legislative instruments: the general data protection regulation (intended to replace directive 95/46/EC) and the data protection directive in the area of law enforcement (intended to replace the 2008 data protection framework decision).

The protection of persons in relation to the processing of their personal data is a fundamental right laid down in the Charter of Fundamental Rights of the EU (Article 8) and in the Treaty on the Functioning of the European Union (Article 16).

General data protection regulation

The general data protection regulation aims at enhancing the level of data protection for individuals whose personal data is processed and increasing business opportunities in the digital single market including through reduced administrative burden.

An enhanced level of data protection

The principles and rules on the processing of personal data of individuals must respect fundamental rights and freedoms, notably the right to protection of personal data. These strengthened data protection rights give data subjects (the individuals whose personal data is being processed) more control over their personal data:

- more specific rules allowing data controllers (those responsible for the processing of data) to process personal data, including through the requirement for the consent of the individuals concerned.
- easier access to their personal data.
- better information about what happens to personal data once it is shared. This includes informing individuals about their privacy policy in clear and plain language, which can also be done via standardised icons.
- a right to erase personal data and "to be forgotten". This enables, for example, subjects to require the removal, without delay, of personal data collected or published on a social network when the individual was still a child.
- if a youngster of below 16 years wishes to use online services, the service provider has to try to verify that parental consent has been given. Member states may lower this age ceiling without going below 13 years.
- a right to portability, facilitating the transmission of personal data from one service provider, such as a social network, to another. This will not only increase data protection rights but also enhance competition among service providers.
- a right to object to the processing of personal data relating to the public interest or to legitimate interests of a controller. This right covers the use of personal date for the purposes of 'profiling'.
- common safeguards covering the processing of personal data for archiving purposes where that is in the public interest and for scientific and historical research or statistical purposes.

To ensure proximity of legal redress, data subjects have the right for a decision of their data protection authority to be reviewed by their national court, irrespective of the member state in which the data controller is established.

Increased business opportunities in the digital single market

The regulation provides for a single set of rules, valid across the EU and applicable both to European and non European companies offering on-line services in the EU. This avoids a situation where conflicting national data protection rules might disrupt the cross-border exchange of data. It also provides for increased cooperation between member states to ensure coherent application of the data protection rules across the EU. This will create fair competition and will encourage companies, especially

small and medium-sized enterprises, to get the most out of the digital single market.

To reduce costs and provide legal certainty, in important cross-border cases where several national supervisory authorities are involved, a single supervisory decision is taken. This **one-stop-shop mechanism** allows a company which is active in several member states to deal only with the data protection authority in the member state of its main establishment. This mechanism also provides for a single decision applicable to the entire EU territory in case of disputes.

With a view to reducing administrative costs, the regulation applies a risk-based approach: data controllers can implement measures according to the risk involved in the data processing operations they perform. Different businesses have different activities and the risks of such activities in terms of privacy can vary. The regulation provides for no one-size-fits all solution: the stronger the risks of the activities for the personal data, the more stringent the obligations.

More and better tools to enforce compliance with the data protection rules

The regulation provides a range of measures to increase the responsibility and accountability of data controllers in order to ensure full compliance with the new data protection rules. Data controllers must implement a number of security measures, including the requirement in certain cases to notify personal data breaches. To future-proof the regulation, the principles of data protection by design and by default are introduced. Public authorities and those companies that perform certain risky data processing must designate a **data protection officer** to ensure compliance with the rules.

Data subjects, and in certain conditions, data protection organisations can lodge a complaint with a supervisory authority or seek judicial remedy in case the data protection rules are not complied with. Data controllers can face maximum fines of up to €20 million or 4% of their global annual turnover.

Guarantees on the transfer of personal data outside the EU

The regulation lays down the rules for transferring personal data to third countries and international organisations. Transfers may take place provided that a number of conditions and safeguards are met, in particular where the Commission has decided that an adequate level of protection exists. New adequacy decisions will have to be reviewed at least every 4 years. Existing adequacy decisions and authorisations remain in force until amended, replaced or repealed.

Data protection directive in the field of law enforcement

This directive is aimed at protecting personal data processed for prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

It is crucial to ensure a consistent and high level of protection of personal data of individuals while at the same time facilitating the exchange of personal data between law enforcement authorities in the different member states.

Broader scope of application

In addition to covering activities aimed at preventing, investigating, detecting and prosecuting criminal offences the new directive has been extended to cover the safeguarding and prevention of threats to public security.

The new directive would apply to both the cross-border processing of personal data as well as the processing of personal data by the police and judicial authorities at purely national level. The framework decision, which will be replaced, covered only cross-border exchange of data.

Data subject's rights

The rules strike a balance between the right to privacy and the need for the police not to reveal that data is being processed at an early stage of an investigation. However, the text lists the information that the data subject is always entitled to receive in order to protect his or her right if they fear that an infringement of their data has taken place.

The new rules will also cover the transfer of personal data to third countries and international organisations.

Compliance

The new directive foresees that a **data protection officer** is appointed to help the competent authorities to ensure compliance with the data protection rules.

Another tool to ensure compliance is impact assessment. Where a type of processing is likely to result in a high risk for the rights and freedoms of individuals the competent authorities must carry out an assessment of the potential impact of a certain processing, in particular when using new technology.

Monitoring and compensation

The text of the directive is aligned with the text of the regulation in order to ensure that in broad terms the same general principles apply. In addition, the rules on the supervisory authority are to a large extent similar because the supervisory authority established in the general data protection regulation can also deal with matters falling under the directive. The new directive would also grant data subjects the right to receive compensation if they have suffered damage as a consequence of a processing that has not respected the rules.

NEXT STEPS

On 17 December, in an extra-ordinary meeting, the European Parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee endorsed the texts agreed in the trilogues. This support enabled Coreper today to confirm the final compromise texts on the regulation and the directive. After a legal-linguistic review of the texts, they will be submitted for adoption by the Council and, subsequently, by the Parliament. The regulation and the directive are likely to enter into force in spring 2018.

Press office - General Secretariat of the Council of the EU
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press