# GDPR goes live: A modern data protection law

Aimed at strengthening citizens' rights uniformly while reducing burdens for companies and public entities, the European General Data Protection Regulation (GDPR) applies fully as of 25 May 2018. The long-awaited (and often feared) law is part of a reform package adopted in 2016 to foster trust in a digital age. The recent revelations on misuses of data show how the underlying values of the GDPR standards are essential for democracy.

## Strengthening individual rights while ensuring the free flow of data

Personal data are increasingly collected and processed – often automatically – for many different purposes. Besides the benefits for society and individuals, data processing raises concerns for individual rights, including 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 avoid possible abuses by those who handle the data, clear and strict rules are necessary. The advance of digital technologies, the emergence of 'Big Data' and of a data-driven society – where almost every daily activity requires the flow and combination of data – made it urgent to update the EU 1995 data protection rules, with new ones, better suited to the digital age.

### A long tradition of strong data protection

The rights to private life and data protection are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights (CFR), binding as EU primary law since the Lisbon Treaty. Consequently, in Europe everyone has the right to personal data protection: data must be processed fairly and for specified purposes, on the basis of the subject's consent or of another legitimate basis laid down by law. Everyone also has the right of access to data concerning them and the right to have it rectified. Compliance with the rules is subject to control by an independent authority.

## GDPR: main changes

Defined as an evolution, rather than a revolution, the 2016 GDPR builds on its 1995 predecessor, Directive 95/46/EC and on the jurisprudence of the Court of Justice (CJEU) which repeatedly confirmed the importance of a high level of data protection for a democratic society. The GDPR (rapporteur: Jan Albrecht, Greens/EFA, Germany) was adopted as part of a wide-ranging reform package, which also includes a directive on data processing for law enforcement purposes. A set of new rules on e-Privacy and on data protection within the EU institutions are (with some delay) also under consideration.

The GDPR promises to improve both the internal market dimension and protection of citizens, by providing greater control over their personal data in the digital era and by establishing legal consistency. While its strict rules are often viewed as a severe challenge penalising companies, which may even threaten to stop serving EU citizens, they are also promoted as an advantage for compliant companies, including SMEs, enabling them to increase users' trust and to compete globally. The underlying idea of the GDPR is to modernise the principles established by the 1995 directive: obligations and sanctions must be taken more seriously now, but they are also scalable (e.g. they may vary based on the violation or on company's size).

The regulation is directly applicable in the Member States, although they have some discretion (e.g. on the age of a consenting child) and the Commission needs to set out details. Consistency across the EU should level the playing field for companies operating in several Member States, allowing them to deal with a single authority and uniform procedures (*one-stop shop*).

### Safeguards

Data are considered personal when they can identify a person (including ID card number, IP address, location data of a phone). Rules do not apply to anonymous/mized data (if anonymisation is irreversible). Data processing is allowed if the conditions indicated are satisfied, i.e. with the subject's informed and unambiguous consent or for other legal grounds (e.g. the performance of a contract; a legal obligation; or legitimate interests, overriding the interests or fundamental rights of the data subject. Also, data must be collected for specified, explicit and legitimate purposes and not further processed in an incompatible way; GDPR generally prohibits the processing of sensitive data, but exceptions are set out.


Author: Shara Monteleone, Members' Research Service
PE 621.873 – May 2018

Besides strengthening existing individual **rights** (increased transparency and easier access to one's own data), the GDPR introduces new ones, like the transfer of personal data from one service provider to another (data portability); to have one's data deleted if there are no legitimate grounds to retain them (right to be forgotten); to object to profiling (as statistical deduction is often used to make predictions about people).

### Increased accountability but also reduced burden for companies

The GDPR applies to all companies operating in the EU, wherever they are based (to non-EU companies too). Companies have to inform individuals about the collection, purposes and use of data and are responsible for demonstrating their compliance with the rules. They have to keep a record of their data-processing activities and must take appropriate technical and organisational measures to make data secure, and inform both individuals and the competent DPA, if data are *accidentally or unlawfully* destroyed, lost or accessed by unauthorised persons, with a risk to individuals' rights ('*breach notification*').

Companies' requirements, *in certain circumstances*, include: designation of a data protection officer, impact assessment, and data protection by design and by default (i.e. 'to embody' data protection rules into a product or service, programming the settings as the most privacy-friendly).

### Sanctions and other enforcement mechanisms

**Fines** *up to* 4 % of a firm's *total worldwide annual turnover* may accompany or replace corrective measures (as warnings or orders) adopted by national supervisory authorities (DPAs) in case of some infringements. As for the **remedies**, data-subjects can lodge a claim in front of empowered DPAs or national courts. At EU level, a new board for national supervisory authorities is established: the EDPB.

The Commission published a communication on GDPR implementation and an online tool for businesses. The Article 29 Working Party also provided guidelines, including on consent, profiling and transparency.

### Data transfers to third countries

Data transfers may take place (as in the 1995 directive) only if the third country can ensure an adequate level of data protection**,** assessed in light of all the circumstances including laws in force. According to the CJEU, this requirement should be read in light of the CFR, which justifies limitations to data protection rights if provided in law, if strictly necessary and proportionate to objectives of general interest. Alternative tools include a simplified process for binding corporate rules; standard clauses approved by the Commission and a certification mechanism. Moreover, it is clear that Europe is influencing the global standards for privacy.

### The Facebook/Cambridge Analytica scandal

Recent revelations about the misuse of users' data, have raised criticism in Europe, and revealed connections between unlawful data processing and disinformation/manipulation of data.

In spring 2018, newspapers reported that Cambridge Analytica (CA), a UK-based political consulting firm, had improperly obtained in 2014 data on 87 million Facebook (FB) users, without their consent. Data collection was initially made via a third-party app that 270 000 FB users were invited to install (voluntarily) for research purposes. Data of friends of friends, collected exponentially, were passed to CA, which used that data to target online voters/users with personalised political ads, allegedly seeking to manipulate their behaviour in the US elections in 2016 (and in the 2016 UK EU membership referendum).

Commissioner Věra Jourová promised an EU-wide investigation, and to leverage, for the future, the measures offered by the GDPR. The need to fully protect citizens' personal data was also stressed at the March European Council. The EP President confirmed commitments to investigate these alleged misuses of data. As FB/CA are certified companies under the EU-US Privacy Shield, the LIBE committee has proposed a draft resolution on the adequacy of this framework. During the EP's April plenary session MEPs called for a strong European position and insistently invited FB's CEO Mark Zuckerberg to appear in the EP to give clarifications. The Article 29 Working Party deemed FB's apologies insufficient and established a Social Media Working Group. The European Data Protection Supervisor, in an opinion on online manipulation and personal data, underlined that what happened was not a mistake, but the result of a predominant business model, that might need to be changed. Finally, some experts see this data misuse not as a data breach, but due to features of FB (and similar). The really big change would be around enforcement: the EU has had long-established rules, but it lacked the teeth to impose compliance. This will finally come with the GDPR.

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. © European Union, 2018.