At a glance
April 2016

Golden Eye: Who rules tomorrow's Europe?

The development of digital technologies has made access to and availability of personal data easier for companies, public authorities and citizens. Keeping control over our personal data means keeping control over our life. Personal data collection and processing are regulated by EU law with the aim of striking a balance between rights to privacy and to data protection and other rights or interests (e.g. freedom of expression, public security).

Data protection as a fundamental right

What are personal data? Any information relating to a person who can be identified, directly or indirectly, by those who handle this information and referring, for instance, to identification number, location data, online identifier or physical or socio-economic factors is personal data. Our data are increasingly collected and processed automatically for different purposes, both commercial and governmental. The development of digital technologies in recent years 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 EU's data protection (DP) regime. This legislation dated back to 1995, when many of today's technologies and services did not exist. The main principles, however, are still valid and are, in fact, strengthened in the 2016 reform.

Data protection is a fundamental right, enshrined in the EU Charter of Fundamental Rights (Article 8), along with the right to privacy (Article 7). EU law must be in line with these principles, but differences in Member States' implementation led to inconsistencies, legal uncertainty and bureaucratic burdens. New rules were thus needed to keep pace with the digitalisation of modern services, commerce, and communications.

Why is it so **important** to protect our data? We can decide whether to share, and where, our data, and once we provide our data to a company or public authority we expect that they make good use of them. The DP framework establishes basic rules to ensure that data are not used without our consent (with limited exceptions), that we are informed about their use, and that data controllers protect them. Being informed means being able to make better decisions on our data. However, in some cases if we refuse to provide data, we will have to forego a specific service. The law establishes strict conditions under which data can be processed, to address asymmetry of powers or information ('Internet giants' know more about us than we know about them). If we fear our data have not been properly used, we can seek remedy from the national DP Authority or a judge. Threats to individuals' rights may derive also from misuse or abuse of personal data: discrimination or restriction of other fundamental rights, like freedom of expression, are at stake. DP is thus instrumental for the exercise of other rights and for the existence of a democratic society. However, DP is not an absolute right, and it may conflict with other over-riding rights and interests (e.g. national security, fight against crime). Therefore EU law sets a series of principles and rules to ensure that the right balance between rights is achieved following the necessity and proportionality principles.

Digital technologies: opportunities and challenges for data protection

While most Europeans access the internet to read news, join social networks, email or shop, the majority are concerned about data being collected without their knowledge (e.g. through mobile apps), and around 70% fear that their data are not safe in companies' hands. While the use (and re-use) of *big data* is seen as a driver of the economy and innovation, its applications (e.g. for facial recognition), may be as remarkable as worrying. This increases the sense of opacity of many digital practices and leads to a perceived loss of control in our lives. Internet giants have often been the object of complaints and sanctions for having decided unilaterally how to process data about unwitting users collected on their platforms, and against the EU standards (e.g. Facebook was recently fined by the Belgian supervisor).

This note has been prepared for the European Youth Event, taking place in Strasbourg in May 2016.

EPRS | European Parliamentary Research Service
Author: Shara Monteleone, **Members' Research Service**
PE 581.976

Improvement in EU data protection: the recent DP reform package

Strengthening citizens' rights to control over their data: the General Data Protection Regulation

Almost five years after the European Commission's proposal, on 14 April 2016 the European Parliament (EP) adopted the long-awaited General Data Protection Regulation, to establish a single, strong set of rules for all Member States (instead of 28 laws). People's personal data will be better protected, regardless of where they are stored, processed or sent – including outside the EU, as often happens on the internet. The Regulation also applies to non-EU companies offering goods or services in the EU or monitoring the online behaviour of individuals.

Citizens would be in control of their data, in particular with a clear and *affirmative consent* requirement (not presumed); increased *transparency* on how data are used (e.g. the use of shorter texts and clearer information is encouraged, in particular through intuitive privacy policies and settings like icons); a *'right to be forgotten*' (unless there are legitimate grounds for retaining data, e.g. freedom of press, an individual may have their data deleted); a right to *data portability*, allowing individuals to transmit their personal data from one service provider to another; a *parental consent* requirement for youngsters to use online services (the age threshold is to be defined by Member States, at between 13 and 16 years); a right to *object* to profiling; a right to know *when data have been hacked*; and *fines* to companies of up to 4% of their annual turnover if they infringe the rules. Data protection *by design and by default,* i.e. embedding data protection values through innovative methods and technical solutions from the beginning, is also an essential principle of the new law. This not only allows individuals to keep control over their data but also encourage innovation, aimed, for instance, at providing encrypted and 'pseudonymised' data that can be used in big data analytics or to find alternative ways to protect *digital natives* (children).

The new rules also benefit **companies** (ensuring the *free flow* of data while safeguarding individuals' rights), thanks to, among other things, reduced bureaucracy: e.g. a company operating in several Member States will only have to deal with a single data protection authority (*one-stop shop*) and is no longer obliged to notify its data processing to a DP authority but to conduct an *impact assessment* of risky cases. For e-communications, including traffic and location data, the ePrivacy Directive should also be reviewed in 2016 in order to ensure a high level of data protection and a level playing field for all market players in the digital world (not just telecoms companies). This may be the time to reconsider instruments like tracking cookies. A public consultation has been launched, and you can have your say.

Data protection should be **effective**, as recent judgments of the Court of Justice of the EU have underlined. For instance, in the *Google Spain* case, a right to delete personal data has been recognised, in *Digital Rights Ireland* the Data Retention Directive was invalided and in the *Schrems* case the protection of EU citizens' data when transferred to third countries was stressed. In this way the Court contributed to the definition of the DP rights that are now included in the reformed legislation, and also directed national case law.

Fighting crime while safeguarding data protection: what a challenge!

On 14 April, the EP also adopted the Directive on data processing in the police and criminal justice sector. This aims to ensure that DP and other fundamental rights of individuals (whether they are a victim, witness, suspect or criminal) are safeguarded consistently, while enabling effective cooperation among law enforcement authorities and facilitating the exchange of data between Member States. While sharing of data by police and law enforcement and the use of sophisticated technologies may be necessary for national security purposes, it must also comply with the principles of necessity, proportionality and legality, ensuring supervision by independent DP authorities and effective judicial remedies (in case of individual complaints). Leaving aside *Minority Report*-like scenarios, at stake is the risk of generalised surveillance and criminalisation ('we are all suspects'), of unjustified invasion of our private lives or of discrimination. The new Directive will help authorities transfer personal data efficiently, guaranteeing oversight mechanisms.

Finally, in April, the EP also voted on the EU PNR Directive, requiring airlines companies to collect and share passenger data for crime-prevention and investigation. Criticism, however, is not lacking, with a possible challenge to the new rules before the Court of Justice expected in the coming years.

The new Regulation's provisions will be *directly* applicable in all EU Member States in two years' time. The two Directives have to be *transposed* into national law, by the same two-year deadline.