Background

Q&A: new EU rules on data protection put the citizen back in the driving seat

[01-06-2016 - 15:50]

New EU data protection legislation aims to create a uniform set of rules across the EU fit for the digital era, improve certainty as to the law and boost trust in the digital single market for citizens and businesses alike. Clear and affirmative consent to data processing, the right to be forgotten and tough fines for firms breaking the rules are some of the new features.

The European Parliament finalised more than four years of negotiations when MEPs passed the legislation in the Civil Liberties Committee on Tuesday 12 April, followed by a vote by the full house on Thursday 14 April.

The overhaul concerns two pieces of legislation: a general regulation on personal data processing in the EU and a directive on data processed by the police and judicial authorities. Together, these make up the data protection package.

The regulation will replace the EU data protection directive which dates from 1995, when the internet was still in its infancy. It will replace the current patchwork of national laws with a single set of rules designed to give citizens more control over their own private information in a digitised world of smart phones, social media, internet banking and global transfers. It also aims to improve certainty as to the law for businesses, so as to boost innovation and the future development of the digital single market. The data protection regulation will strengthen trust and provide for a high level of protection for all individuals across the EU in whatever circumstances their personal data are processed, except for law enforcement purposes (which are covered by the directive), and will also apply to firms outside Europe targeting EU consumers.

The data protection directive covers data processing by the police and criminal justice sector. It aims to ensure that the data of victims, witnesses, and crime suspects, are duly protected in criminal investigations and law enforcement actions. At the same time, more harmonised laws should also facilitate cross-border cooperation among police forces and prosecutors, enabling them to fight crime and terrorism more effectively across Europe.

After the Council formally approved the data protection package at its first reading on Friday 8 April, Parliament finally completed more than four years of negotiations that began when the Commission presented its proposals in January 2012. Parliament voted its first-reading position in March 2014, but had to wait for more than a year for member states to agree on their common negotiating position before the three-way-talks between Parliament, Council and Commission could begin in June 2015. In the case of the directive, the Council agreed a compromise on its negotiating mandate in October 2015.

An informal agreement was reached on 15 December 2015, and endorsed by Parliament and Council on 17 and 18 December respectively. Since then, Parliament has repeatedly called on the Council to finalise its work on the texts to allow the stronger data protection requirements to enter into force swiftly. In particular, a majority of MEPs has consistently stressed the urgent and indispensable need to guarantee a sufficient level of data protection, as set out by the data protection directive, before allowing the bulk collection of flight passenger data envisaged by the EU Passenger Name Record (PNR) directive, which is also to be put to a vote at the April Strasbourg session.

The plenary vote marked the final step in the legislative procedure. The data protection regulation will enter into force 20 days after its publication in the EU Official Journal, and become directly applicable in all member states two years after this date. Member states will also have two years to transpose the provisions of the directive into their national laws.

Contact

Rikke ULDALL
BXL: (+32) 2 28 42976
STR: (+33) 3 881 72033
PORT: (+32) 498 98 32 57
EMAIL: libe-press@europarl.europa.eu
TWITTER: EP_Justice

What does the "data protection package" consist of?

The data protection reform package consists of two laws: a general **regulation** covering the bulk of personal data processing in the EU and a **directive** on processing data to prevent, investigate, detect or prosecute criminal offences or enforce criminal penalties.

The regulation updates the principles set out in a 1995 directive, so as to keep pace with major changes in data processing brought about by the internet. It would cover, for example, data processed on the internet, e.g. for social networks, online shopping and e-banking services, and offline, e.g. for hospital and university registers, company registers of clients and personal data held for research purposes. The lead MEP for the draft regulation is Jan Philipp Albrecht (Greens/EFA, DE).

The directive replaces a 2008 framework decision (2008/977/JHA) on cross-border data processing in police and judicial cooperation within the EU. It is intended to protect both domestic and cross-border transfers of data, which is not the case today. It also sets a high standard of data protection for citizens. The lead MEP for the directive was Marju Lauristin (S&D, ET).

The data protection package is a key enabler of the Digital Single Market and the EU Agenda on Security.

What will the rules in the new data protection regulation entail?

The regulation updates and modernises the principles enshrined in the 1995 data protection directive to guarantee privacy rights. It focuses on: reinforcing individuals' rights, strengthening the EU internal market, improving enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards. The reform is an essential step to strengthen EU citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies.

The new rules will give individuals greater control over their personal data in the following ways.

The right to be forgotten (Article 17)

Any person will have the right to be “forgotten”/have his or her personal data erased when he or shel no longer wants the data to be processed, provided there are no legitimate reasons for retaining it.

To enforce this right, if a person asks an internet company to erase his/her data, the company should also forward the request to any others that replicate the data. However, this right would be restricted in some cases, for instance when the data is needed for historical, statistical and scientific purposes, for public health reasons or to exercise the right to freedom of expression. Also, the right to be forgotten would not apply when the retention of personal data is necessary to fulfil a contract or is required by law.

Better control over who holds one's private data (Article 7)

The person concerned (data subject) will have to give **clear and affirmative consent** to the processing of his or her private data, i.e. giving consent will entail an active step by the individual. This could for example mean ticking a box when visiting an internet website or another action or statement clearly indicating acceptance of the proposed processing of the personal data. Silence, pre-ticked boxes or inactivity will thus not constitute consent. In future, it should also be as easy for a person to withdraw consent as to give it.

The right to switch one's personal data to another service provider (Article 20)

Under the new rules, any person will have the right to “data portability” to make it easier for individuals to switch their personal data between service providers. For example, this right should allow a user to switch to another email provider without losing contacts or previous emails. This right will not only give individuals more control over their data, but also stimulate competition in the digital single market.

The right to be informed in clear and plain language (Articles 12, 13, 14)

MEPs have insisted that the new rules will put an end to “small print” privacy policies. Information should be given in clear and plain language before the data is collected.

The right to know if your data has been hacked (Articles 33 and 34)

Companies and organisations will be required to notify the national supervisory authority of serious data breaches as soon as possible, so that users can take appropriate measures.

Clear limits on the use of profiling (Article 21)

The new rules set limits to the use of "profiling", a technique used to analyse or predict a person's performance at work, economic situation, location, health, preferences, reliability or behaviour based on the automated processing of his/her personal data.

Under the regulation, profiling would, as a general rule, only be allowed with the consent of the person concerned, where permitted by law or when needed to pursue a contract.

MEPs also insisted that profiling should not lead to discrimination or be based solely on sensitive data (i.e. data revealing, inter alia, ethnic origin, political opinions, religion, sexual orientation, genetic or biometric data, administrative sanctions or suspected offences).

Also, profiling should not be based solely on automated processing and should comprise human assessment, including an expectation of the decision to be reached after such an assessment. This could affect the way in which creditworthiness is evaluated, for example.

Special protection for children (Article 8)

The new rules provide for special safeguards for children in some areas, as they may be less aware of risks and consequences related to sharing their personal data. For instance, they will have a clearer right to be forgotten.

The rules also say that children below a certain age will need their parents' permission ("parental consent") to open an account on social media such as Facebook, Instagram or Snapchat, as is already the case in most EU countries today. The age threshold is for member states to define within a range of 13 to 16 years.

This flexible threshold was a compromise reached during negotiations to ensure that member states are free to maintain the rules that they are already applying today. Parliament would have preferred the age limit for parental consent to be 13 across the EU (as initially also proposed also by the European Commission).

The aim of this specific provision is to protect children from being pressured to share personal data without fully realising the consequences. It will not prevent teenagers from using the internet to get information, advice, education etc. Moreover, the rules specify that children below the age limit will not need to ask their parents' permission to make use of counselling or preventive services offered directly to children.

Privacy as norm

In future, companies will have to design defaults and products such that as little personal data as possible are collected and processed. "Privacy by design" or default should become an essential principle and will incentivise businesses to innovate and develop new ideas, methods and technologies for security and protection of personal data.

What are the benefits for businesses?

The reform aims to make the rules clearer and more consistent by replacing the current patchwork of national laws with one, common EU-law. The likely benefits are estimated at €2.3 billion per year, says the European Commission.

A new **one-stop-shop** for businesses will mean that firms will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for companies to do business in the EU. At the same time, this will also have an impact on the oversight of internet giants with offices in several EU countries.

Furthermore, **the rules will apply to all companies targeting EU consumers**, regardless of whether they are established inside or outside the EU. The regulation will make it clear that firms based outside of Europe will have to follow the same rules when they offer goods or services on the EU market. This will help to create a level playing field for all companies operating in the EU.

By having one rule instead of 28, the EU's data protection reform will also help **small and medium-sized enterprises** break into new markets. In a number of cases, the obligations of data controllers and processors are adjusted to the size of the business and/or the nature of the data being processed so as to avoid creating red tape and disproportionate burdens for smaller firms.

How will the new rules be enforced?

To ensure proper enforcement of the new data protection rules the reform will both step up the powers of data protection officers and allow for substantial fines in the event of breaches.

Firms will have to appoint a data protection officer if they are handling significant amounts of sensitive data or monitoring the behaviour of many consumers. Firms whose core business activities are not data processing will be exempt from this obligation, so as to avoid creating red tape.

Fines of up to 4% of firms' total worldwide turnover should constitute a real deterrent to breaking the rules.

What will the new directive on data exchanges in the law enforcement sector mean?

The directive on data transfers for policing and judicial purposes will set high standards of data protection so as to protect citizens' rights and freedoms whilst at the same time enabling police forces across Europe to work together faster and more efficiently to counter serious crime and terrorism.

It applies to the law enforcement sector the same data protection rules as those of the regulation, with necessary adaptions to the sector’s specificities. It innovates by substantially harmonising the EU’s various national methods of processing data for law enforcement purposes and will also for the first time set minimum protection standards for data transfers within each member state.

EU countries may set higher standards than those enshrined in the directive if they so wish.

How will the rules protect individuals?

The directive protects individuals whose data is processed for the purpose of prevention, investigation, detection or prosecution of criminal offences. The safeguards will apply to everyone, whether victim, criminal or witness and sets out clear rights for individuals.

All law enforcement processing in the EU must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals. Everyone's personal data should be processed lawfully, fairly and only for a specific purpose. Supervision is to be ensured by independent national data protection authorities with enforcement powers.

The rules will apply both domestically, within member states, and across borders within the EU. The framework decision, which will be replaced, covered only cross-border exchanges of data. The directive also provides robust rules for the transfer of personal data to third countries and international organisations to ensure that such transfers take place with an adequate level of data protection.

How will the rules affect cooperation in criminal law enforcement?

Having the same law across the EU will make it easier for criminal law enforcement authorities to work together in exchanging information, thus creating conditions for smoother and more effective crime prevention.

The directive also complements recent agreements on a new Europol regulation and the directive establishing a system collecting flight passenger data in the EU (EU PNR) by setting high, uniform standards on data transfers for law enforcement purposes.

Facts and figures

The Civil Liberties Committee tabled a record number of 3,133 amendments to the Commission's proposal for a regulation. These, plus the amendments tabled in the opinions of the Industry Committee (417), the Internal Market Committee (226), the Employment Committee (27) and the Legal Affairs Committee (196), make a total of **3,999 amendments.** This was the highest number of amendments ever tabled in Parliament to **a single legislativefile.**

Parliament's political groups negotiated 91 compromise amendments, combining those already tabled, in order to make it easier to vote on the regulation.

The Civil Liberties Committee tabled 673 amendments to the draft directive. These, plus the amendments tabled by the Legal Affairs Committee in its opinion (98), make a total of 771 amendments.

Parliament's political groups negotiated 64 compromise amendments, combining those already tabled, in order to make it easier to vote on the directive.

The voting list for the regulation was 261 pages long and the one for the directive ran to 57 pages (making a total of 318 pages for the whole package).

By the time of the full Parliament voted in March 2014, the data protection reforms had been debated for 20 months. The committee's official debates alone accounted for some 30 hours. Informal negotiations among political groups took around 250 hours.

Who are the key MEPs dealing with this reform?

- Jan Philipp Albrecht (Greens/EFA, DE) was the rapporteur for the regulation
- Marju Lauristin (S&D, ET) was the rapporteur for the directive.

Parliament's negotiating team for the **regulation** were Civil Liberties Committee chair Claude Moraes, the rapporteur, Jan Philipp Albrecht, and shadow rapporteurs Axel Voss (EPP; DE), Marju Lauristin (S&D, ET), Timothy Kirkhope (ECR, UK), Sophia in't Veld (ALDE, NL), Cornelia Ernst (GUE/NGL, DE) and Kristina Winberg (EFDD, SV). The author of the opinion of the industry committee, Sean Kelly (EPP,IE), and of the internal market committee, Lara COMI (EPP,IT), also attended the trialogues.

Parliament's negotiating team for the **directive** were Civil Liberties Committee chair Claude Moraes, the rapporteur, Marju Lauristin (S&D, ET), and shadow rapporteurs Axel Voss (EPP, DE),Timothy Kirkhope (ECR, UK), Sophia in't Veld (ALDE, NL), Cornelia Ernst (GUE, DE), Jan Philipp Albrecht (Greens, DE) and Kristina Winberg (EFDD, SV).

Further information

- Profile of rapporteur Jan Philipp Albrecht (Greens/EFA, DE) – regulation
- Profile of rapporteur Dimitrios Droutsas (S&D, EL) – directive
- Profile of rapporteur for opinion Seán Kelly (EPP, IE) – Industry Committee
- Profile of rapporteur for opinion Lara Comi (EPP, IT) – Internal Market Committee
- Profile of rapporteur for opinion Nadja Hirsch (ALDE, DE) – Employment Committee
- Profile of rapporteur for opinion Marielle Gallo (EPP, FR) – Legal Affairs Committee
- Profile of rapporteur for opinion (directive), Axel Voss (EPP, DE) - Legal Affairs Committee

Next steps

Parliament's plenary vote on Thursday 14 April marked the end of the legislative procedure on both the data protection regulation and the directive.

The regulation enters into force 20 days after its publication in the EU Official Journal on 4 May 2016. Its provisions will be directly applicable in all member states two years after this date.

Member states will have two years from 4 May 2016 to transpose the directive's provisions into into national law.

Due to UK and Ireland's special status regarding Justice and Home Affairs legislation, the directive's provisions will only apply in these countries to a limited extent, that is only in the areas where the UK and Ireland have “opted in” to other laws on police and judicial cooperation. Outside of these areas, UK and Ireland will not be bound by the directive.

Denmark will be able to decide within six months after the final adoption of the directive, whether it wants to implement it in its national law.