European Parliament

Background

# Q&A on EU data protection reform

[24-06-2015 - 12:40]

**The growing globalisation of data flows, via social networks, cloud computing, search engines, location-based services, etc, increases the risk that people can lose control of their own data. Civil liberties MEPs adopted their position on a major overhaul of current EU data protection rules on 21 October 2013.**

**This overhaul seeks to put people in control of their personal data, build trust in social media and online shopping and upgrade the protection of data processed by the police and judicial authorities.**

**EU member countries approved their negotiating position on the new EU data protection regulation on 15 June 2015. This means that Parliament, the Council and the Commission can now start the first round of three-way talks aimed at striking a final agreement on the regulation. These talks will begin on Wednesday, 24 June 2015.**

This general regulation on personal data processing in the EU will replace the current patchwork of national laws with a single set of rules, which should make it easier for companies to operate across the EU while at the same time strengthening citizens' rights.

The EU's current data protection laws date from 1995, before the internet came into widespread use, and do not cover data processed for law enforcement purposes. Today, 250 million people use the internet daily in Europe. New rules will update the existing legal principles and apply them to the new online environment, to ensure effective protection of the fundamental right to data protection and improve legal certainty for companies.

The changes made on 21 October 2013 by the civil liberties, justice and home affairs committee to the European Commission's proposals for a package of legislation constitute Parliament's mandate to start negotiations with the Council on the final version of the legislation. The full Parliament confirmed the committee's texts in a vote on 12 March 2014.

Parliament then had to wait for member states to agree a "general approach" among themselves in order for final talks to start.MEPs repeatedly called on the Council to move forward on the package of laws, stressing the need to update EU data protection rules without further delay, so as to give citizens the standards of data protection needed in the digital era.

They have also underlined the need to set a uniform standard for data protection in all EU legislation, especially in the European Police Office (EUROPOL) regulation, currently under negotiation, and in an EU passenger name record scheme.

Now that the Council has a common position on the EU data protection regulation (agreed on 15 June 2015), Parliament, the Council and the Commission can start discussions on that. Their first trialogue meeting is scheduled for 24 June. Negotiators hope to be able to reach a final agreement on the package by the end of 2015. However, member states still have to agree a general approach on the other part of the package, namely the directive on data processed in criminal proceedings.

**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 draft 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 draft 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 draft directive seeks to replace a 2008 framework decision on cross-border data processing in police and judicial cooperation. It is intended to protect both domestic and cross-border transfers of data, which is not the case today. It also sets a high level of data protection for citizens. The lead MEP for the draft directive is Marju Lauristin (S&D, ET).

## What are the key issues for Parliament?

Parliament has set out its position on the whole package of data protection reform.

### The regulation

Here is an overview of some of Parliament's key proposals for the **regulation:**

**Data transfers to non-EU countries (Article 43a)**

The rules voted on by Parliament govern transfers of personal data to third countries. If a third country asks a firm (e.g. a search engine, social network or cloud provider) to disclose personal data processed in the EU, the firm would have to get permission from the national data protection authority and inform the person concerned before transferring any data.

**Penalties for companies (Article 79)**

If the rules are infringed, MEPs say the data protection authorities should have to apply at least one of the following penalties:

- a written warning, in the event of less serious breaches;
- a regular periodic data protection audit; or
- for companies, a fine up to €100 million or 5% of annual worldwide turnover, whichever is greater (the Commission proposed up to €1 million or 2% of annual worldwide turnover).

When imposing these penalties, the data protection authorities would have to take into account aggravating factors such as the duration of the breach, its negligent or repetitive character, willingness to cooperate and the amount of damage done.

**Right to erasure (Article 17)**

Parliament says any person (data subject) should have the right to have their personal data erased if a) the data processing does not comply with EU rules; b) the data are no longer necessary for the purposes for which they were collected; or c) the person objects or withdraws his/her consent for the processing of his/her personal data.

Furthermore, 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. This "right to erasure" builds on what is outlined in the 1995 directive and in the Commission proposal.

However, this right would be restricted in some cases, for instance when the data is needed for historical, statistical and scientific research purposes, for public health reasons or to exercise the right to freedom of expression. Also, the right to erasure would not apply when the retention of personal data is necessary to fulfil a contract or is required by law.

The "right to erasure" would cover the "right to be forgotten" proposed by the

Commission.

**Explicit consent (Article 7)**

Parliament says that where processing is based on consent, a company should process personal data only after obtaining clear permission from the data subject, who should be able to withdraw his/her consent at any time. A person's consent means "any freely given, specific, informed and explicit indication of his/her wishes, either by a statement or by a clear affirmative action". The Council, in its negotiating brief, proposes to use the vaguer term "unambiguous consent" which MEPs find too unclear and open to interpretation.

MEPs retained the Commission's proposal. They also stipulate that the execution of a contract or the provision of a service cannot be made conditional upon consent to processing personal data that is not strictly needed for the completion of that contract or service.

Furthermore, according to Parliament's position, the consent should lose its effect as soon as the processing of personal data is no longer needed for the initial purpose for which it was collected. MEPs also stipulate that withdrawing consent must be as easy as giving it.

**Clear and plain language, right to information**

To make it easier for people to give their informed consent, data controllers should use clear, concise, plain language when explaining their privacy policies, and especially when providing any information addressed specifically to a child, MEPs say (Article 11).

When collecting personal data, the controller should explain to the data subject whether his/her personal information will be transferred to commercial third parties, sold, rented out or encrypted. They should also state whether the personal data is being collected and/or will be retained beyond the minimum time needed for the specific purpose of the processing or for different purposes. This should be done using easily understandable

texts and symbols, MEPs add (Article 13a).

The data controller would also be required to inform the person about various aspects of the data processing, such as the period of storage, the recipients of the personal data and the possible existence of profiling, as well as the data subject's rights of access, rectification and erasure of the data and right to lodge a complaint with a data protection authority. (Article 14).

**Profiling (Article 20)**

The proposal sets limits to "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 changes proposed by MEPs, profiling, as a general rule, would only be allowed with the consent of the person concerned, where permitted by law or when needed to pursue a contract. The Parliament text also clarifies 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).

Parliament also makes clear that profiling should not be based solely on automated processing and should comprise human assessment, including an explanation of the decision reached after such an assessment. This could affect the way in which creditworthiness is evaluated, for example.

**Data portability**

Under the Commission proposal, any person would have the right to ask e.g. an email service provider or a social network to provide a copy of all his/her data in an electronic, commonly used format, to be transferred to another provider or service (so-called right to "data portability", Article 18).

MEPs propose merging the right to data portability with the right to data access (Article 15) and stress that, for personal information processed by electronic means, the controller should provide a copy of these data "in an electronic and interoperable format". This would allow users to switch email providers without losing contacts or previous emails, for instance. Where technically feasible and at the request of the data subject, the data would be transferred directly from controller to controller (e.g. from email provider to email provider).

**Data protection officer (Article 35)**

Public institutions, companies processing the data of more than 5,000 people in a year

and organisations whose core activities involve processing sensitive data or systematically monitoring people would be required to appoint a data protection officer (DPO). This proposal is based on the German model.

MEPs' amendments change the criteria for appointing a DPO. For exampleone criterion used would be not how many employees a company has (the Commission suggested at least 250), but rather how many people's data it collects. Also, DPOs should be appointed for at least four years in the case of employees and two in the case of external contractors. The Commission proposed two years in both cases.

DPOs should be in a position to perform their duties independently and enjoy special protection against dismissal, says Parliament. Council, in its negotiating brief, suggests leaving it up to member states to decide whether or not to establish DPOs.

**Right to complain (Article 54a)**

Under MEPs' amendments, those persons whose personal data is processed by a controller (e.g. an internet company) in another EU member state should be able to complain to the data protection authority of his/her choice (that of the country where the company is based or the one in his/her own country). This should make it easier for citizens to lodge complaints in their own language.

**Stronger and more independent Data Protection Authorities**

MEPs reinforce the independence of the Data Protection Authorities (DPAs) and clarify their powers of intervention In line with Article 16 of the EU Treaty and with the case law of the Court of Justice of the EU.

**One-stop shop and consistency mechanism**

A key innovation of the regulation is that it establishes a single competent authority for all the processing activities of a data controller or processor in the EU. The DPA of the country where the controller has its main establishment would have the lead when it comes to taking measures with regard to that controller. The DPA would consult other national data protection authorities involved (eg that of the citizen lodging a complaint). This would have an impact on the oversight of internet giants with offices in several EU countries.

In the event of disagreement, there would be a "consistency mechanism" in which the European Data Protection Board (a body that would coordinate DPAs) would be involved.

## The directive

Here is an overview of some of Parliament's key proposals for the **directive:**

Whereas the general regulation will apply directly in member states, the directive on data processed by police and judicial authorities to prevent, investigate, detect or prosecute criminal offences or enforce criminal penalties will need to be transposed into national laws. EU countries may set higher standards than those enshrined in the directive.

Member states have yet to agree their negotiating brief for the directive. MEPs insist that it is important to remove disparities between member states' existing laws in this field and to close loopholes. To this end, Parliament wants this directive to be dealt with at the same time as the regulation (as a package).

Parliament's negotiating mandate says that a number of concepts envisaged in the regulation, such as profiling, explicit consent, using clear, simple language and appointing a data protection officer, should also apply to the directive.

MEPs say it should only be possible to transfer personal data to third countries or international organisations if the transfer is needed for the same purposes as those provided for in the directive; if the controller in the foreign country/organisation is a public authority; and if the level of data protection provided is guaranteed to be the same as in the directive. Transfers would also be allowed if the Commission decides that the foreign country/organisation provides a proper level of data protection or where appropriate safeguards are established in a legally binding instrument (Article 33).

Member states should ensure, says Parliament, that clear, easily understandable information is given to a person regarding the processing of his/her data and key rights, such as the right of access, rectification and erasure of their data; the right to lodge a complaint and to go to Court; and the right to compensation in the event of unlawful processing. Such rights should be exercised free of charge (Article 9a, Articles 11-17).

Data must be dealt with in such a way that it is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage (Article 4).

Personal data should not be processed for purposes other than those for which it was collected. It must be deleted if it is no longer necessary for those initial purposes, say MEPs, adding that member states must ensure that time limits are set for the erasure of personal data (Article 7a, Article 4).

Profiling activities to single out a person without the suspicion that he/she has committed or will commit a crime would be possible only if strictly needed for the investigation of a serious crime or to prevent an imminent threat to public security or the life of persons (Article 9).

As a general rule, law enforcement authorities would have access to the data of persons convicted for a crime, suspects (on reasonable grounds), victims and other persons connected to a criminal investigation, such as witnesses. The data of other persons would be processed only for as long as necessary for the investigation or for targeted, preventive purposes (Article 5).

MEPs introduce strict limits for the use of sensitive data (Article 8). Genetic data should be processed only to prevent a threat to public security or a specific criminal offence (Article 8a).

## Key definitions

### *Personal data*

"Personal data" is any information concerning a person's private, professional or public life. It may be a name, a photo, an email address, bank details his/her posts on social networks, medical information or his/her computer's IP address.

### *Data controller*

"Data controllers" decide on the conditions, purposes and manner in which personal data is processed. They may be individuals, firms or public authorities. Examples of individuals who act as data controllers include doctors, pharmacists and politicians, when they keep data on their patients, clients and constituents.

### *Data processor*

"Data processors" process personal information on behalf of and under the authority of data controllers but do not take decisions on the conditions, purposes and means of the processing (outsourcers). For example, payroll companies, accountants and market research companies are data processors when they process personal information on behalf of others (e.g. other companies or public authorities, which would be data controllers in such cases). However, if they decide on conditions or purposes or act beyond the instructions of the controllers, they become controllers for that specific processing activity.

### *Data subject*

Personal data are used to identify a natural person. That person is the "data subject".

## 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 is 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 is 261 pages long and the one for the directive runs 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.

Parliament's negotiating mandate for the regulation was adopted by 51 votes to 1, with 3 abstentions.

Parliament's negotiating mandate for the directive was adopted by 47 votes to 4, with 1 abstention.

## Who are the key MEPs dealing with this reform?

### Who are the key MEPs dealing with this reform?

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

Parliament's negotiating team for the **regulation** will be formed by the chair of the civil liberties committee, 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), will also attend the trialogues.

Parliament's negotiating team for the **directive** will be formed by the chair of the civil liberties committee, 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).

## What happens next?

Parliament, the Council and the Commission will now meet in three-way talks in order to seek a final agreement on the data protection regulation before the end of 2015.

Member states still have to agree their negotiating brief for the directive. MEPs urge the EU countries to come to an agreement on this by October 2015 and stress that the regulation and the directive should be negotiated as a package.

Parliament's aim is to reach agreement on both the regulation and the directive before the end of 2015.

## Key dates

### Key dates

- 25.01.2012: Commission proposals for a regulation and a directive
- 29.05.2012: Workshop organised by the civil liberties committee
- 9 & 10.10.2012: Interparliamentary committee meeting - "Building trust in a digital and global world"
- 10.01.2013: Presentation of the draft reports by Mr Albrecht and Mr Droutsas
- 23.01.2013: Internal market committee vote on its opinion
- 20.02.2013: Industry committee vote on its opinion
- 21.02.2013: employment committee vote on its opinion
- 27.02.2013: Deadline for presenting amendments in the civil liberties committee
- 19.03.2013: Legal affairs committee vote on its opinion
- 20.03.2013: First discussion on the amendments in the civil liberties committee
- 6 & 7.05.2013: Second discussion on the amendments in the civil liberties committee
- 9.07.2013: Presentation of the state of play in negotiations between political groups
- 21.10.2013: Civil liberties committee vote on its negotiating mandate
- 12.03.2014: Plenary vote, first reading

- 06.2015: Council approval of its general approach on the regulation
- 06.2015: First trialogue meeting between Parliament, Council and Commission
- Second half of 2015: Parliament and Council negotiations
- Before end of 2015: Parliament and Council agreement