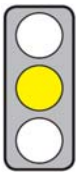
GENERAL DATA PROTECTION REGULATION

cep **Policy Brief** No. 2012-36 of 03 September 2012

KEY ISSUES

Objective of the Regulation: The Commission wishes to reform the data protection law for the internet age.

Parties affected: All citizens and companies, public authorities.



Pros: Harmonising data protection law and assigning EU-wide competence to a national public authority reduces the costs of the companies affected and creates a level playing field.

Cons: (1) The design and the number of the powers conferred upon the Commission are not acceptable in terms of the division of powers. Decisions which are essential for one branch of law are to be taken by the European legislator itself.

(2) The rules regarding the invalidity of the consent are insufficiently concrete; moreover, here, too, the necessity to process data related to health should be taken into account.

(3) The rules regarding employees' data protection do not serve legal certainty.

CONTENT

Title

Proposal COM(2012) 11of 25 January 2012 for a **Regulation** of the European Parliament and of the Council on the **protection of individuals with regard to the processing of personal data** and on the free movement of such data **(General Data Protection Regulation)**

Brief Summary

Note: The articles and pages quoted refer to the Proposal COM(2012) 11.

- **Background and objective**
  - EU data protection law was established in the mid 90s (Data Protection Directive 95/46/EC, as last amended through the Regulation (EC) No. 1882/2003) – in other words, when the internet was still "in its infancy" [COM(2012) 9, p. 3].
  - EU data protection law is to be adapted to the internet age. Its reform mainly focuses on a "modern, strong, consistent and comprehensive data protection framework for the European Union" [COM(2012) 9, p. 12] through full harmonisation, whose key component is the new General Data Protection Regulation (hereinafter referred to as: GDPR).
- **Scope**
  - Basically, the material scope covers any automated processing of personal data and their storage in filing systems (Art. 2 (1); exemptions: Art. 2 (2)).
  - The personal scope applies in particular to:
    - the "controller", who is anyone who alone or jointly with others determines the purposes, conditions and means of the processing of personal data (Art. 4 (5));
    - the "processor", who is anyone who processes personal data on behalf of the controller (Art. 4 (6)).
  - The territorial scope applies in particular to:
    - controllers established in the EU (Art. 3 (1)), irrespective of whether or not the data are processed within or outside the EU (Recital No. 19);
    - controllers established outside the EU (Art. 3 (2)), provided
      - the personal data of "data subjects residing in the Union" (not only: citizens of the Union, Art. 9 TEU) are processed and
      - the data processing activities are "related" to offering goods or services to such data subjects in the Union or to monitor their behaviour, namely by creating user profiles (Recital No. 21; so-called profiling).
  - The Member States may under certain conditions continue to legislate on processing, inter alia:
    - of data related to health (Art. 81 in conjunction with Art. 9 (2) lit. h);
    - of employees' personal data by employers "within the limits of this Regulation" (Art. 82);
    - through public authorities or in connection with services of general interest (cf. Art. 6 (1) lit. e, (3) lit. b, Recital No. 36).
- **Lawfulness of data processing**
  - The processing of personal data is lawful (Art. 6 (1) lit. b–f):
    - where it is required for completion of a contract to which the data subject is party;
    - for fulfilling a legal obligation of the controller;

Author Oliver Sauer | sauer@cep.eu
CEP | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-105 | www.cep.eu

- where the "vital" interests of the data subject require it to be so;
- if it is necessary for the performance of public duties;
- where it is otherwise "necessary" for the purposes of the "legitimate interests" of the controller and the interests or fundamental rights and freedoms of the data subject do not overweigh.

– The processing of so-called sensitive data such as personal data revealing religion or belief, health or criminal convictions (Art. 9 (1)) is in principle unlawful, though, for example, in the case of an employment contract (Art. 9 (2) lit. b) or before public authorities (cf. Art. 9 (2) lit. g), something other may apply.

► **Consent to personal data processing**

– The processing of personal data is in principle also lawful upon the consent of the data subject (Art. 6 (1) lit. a).

– By way of exception, consent does not legitimate the processing of personal data where:
- there is a "significant imbalance" between the position of the data subject and the controller (Art. 7 (4)), "especially" in a "situation of dependence", e.g. from the employee to the employer (Recital No. 34);
- the processing of data is generally prohibited (cf. Art. 9 (1) and EU law beyond the GDPR or national law excludes a consent (Art. 9 (2) lit. a).

– The burden of proof for giving consent is borne by the controller (Art. 7 (1)). In the case of a written declaration, the consent must stand out clearly from the rest of the text (Art. 7 (2)).

► **Executing data processing**

– Data processing includes, inter alia, the following obligations:
- the application of technical procedures which protect the data subjects as far as possible ("data protection by design"), such as "data protection by default", e.g. for social networks (Art. 23);
- the (ongoing) comprehensive documentation (details: Art. 28) which replaces the general (prior) notification of data processing to the supervisory authority (Art. 18, 19 of Directive 95/46/EC); it does not apply to companies with less than 250 employees which only process data as an activity "ancillary" to their main activities (Art. 28 (4) lit. b);
- compliance with data protection standards (details: Art. 30);
- notifying a data protection breach to the supervisory authority (Art. 31) and to the data subjects (Art. 32).
- "data protection impact assessments" in particularly risky constellations (details: Art. 33);
- the designation of a data protection officer (Art. 35) where
  - data processing is carried out by enterprises employing 250 employees and more;
  - the "core activities" of the controller require regular and systematic "monitoring of data subjects" (different from explanation, p. 12 and Recital No. 75: where the "processing operations" require a regular and systematic "monitoring");
  - data processing is carried out by public authorities or public institutions.

– The data subject's rights include, inter alia:
- The "right to be forgotten and to erasure": the data subjects may under certain conditions require the erasure of their personal data and request the abstention from further dissemination of such data (Art. 17 (1) and "all reasonable steps" to inform third parties (Art. 17 (2)).
- The "right to data portability": the data subject has the right to obtain from the controller a copy of their personal data "in an electronic format which is commonly used", for instance to transfer them to another provider e.g. of internet services (details: Art. 18).
- The right to object, which can engender a burden of justification for the controller (details: Art. 19).

– The addressee of obligations is normally the controller, but depending on the obligation also the processor.

► **National data protection authorities**

– Each Member State must undertake to establish an effective data protection supervision (Art. 46 (1)).

– In exercising its duties (Art. 52) and the powers conferred upon it (Art. 53), the supervisory authority is to act with "complete" independence (Art. 47 (1)). In particular, it is not subject to instructions in any form whatsoever (cf. Art. 47 (2)).

– In principle, each supervisory authority is (only) competent on the territory of its own state (Art. 51 (1)). If a controller or processor has establishments in more than one Member State, the authority of the Member State with the "main establishment" (Art. 4 (13), Recital No. 27) is also competent in the other Member States (Art. 51 (2); so-called "one-stop shop" principle).

► **Legal protection**

– The following have the right to lodge a complaint with the supervisory authority:
- every affected natural person (Art. 73 (1));
- bodies, organisations or associations whose aim is to protect data on behalf of affected natural persons (Art. 73 (2)) and in their own name (Art. 73 (3)).

– The following have the right to judicial remedy against a supervisory authority:
- in principle every affected natural or legal person (cf. Art. 74 (1), (2));
- bodies, organisations or associations whose aim is to protect data on behalf of affected natural persons (Art. 76 (1), Art. 73 (2) in conjunction with Art. 74).

– The following have the right to judicial remedy against controllers and processors:
  - every affected natural person (Art. 75 (1));
  - bodies, organisations or associations whose aim is to protect data on behalf of affected natural persons (Art. 76 (1), 73 (2) in conjunction with Art. 75).

► **Liabilities and sanctions**
– Controllers and processors are jointly and severally liable, including the option of exoneration (Art. 77).
– The Member States lay down the rules on penalties, applicable to infringements (Art. 78 (1)).
– Every supervisory authority is empowered to impose direct fines (Art. 79 (1)). Depending on the extent of the infringement, these can be for a sum of up to 1.000.000 Euro, or in the case of enterprises, 2% of global annual turnover (Details: Art. 79 (3)–(6)).

► **Regulatory powers of the Commission** (see CEP Overview)
The Regulation contains 26 powers to adopt delegated legal acts (Art. 290 TFEU; see CEP Analysis) and 25 powers to adopt implementing acts (Art. 291 TFEU; see CEP Policy Brief).

Statement on Subsidiarity by the Commission

According to the Commission, standardised EU-wide data protection is necessary in order to enable the cross-border flows of personal data, at the same time as guaranteeing for all data subjects effective data protection throughout the EU (p. 6).

Policy Context

The data protection package of January 2012 comprises a Communication [COM(2012) 9], the present Regulation, which mainly replaces the existing Data Protection Directive 95/46/EC (Art. 88) and sets the "general EU framework for data protection" [see COM(2012) 9, p. 4], and the Directive [COM(2012) 10] on police and judicial cooperation in criminal matters (PJCCM), which replaces the existing Framework Decision 2008/977/JI.

Legislative procedure

25 January 2012	Adoption by Commission
16 February 2012	Delegation to the Committees Since then: reasoned opinions on subsidiarity by the French Senate (6 March 2012), the Belgian House of Representatives (27 March 2012), the German Bundesrat (30 March 2012; see Bundesrats-Drucksache 52/12), the Swedish Riksdag (30 March 2012) and the Italian Chamber of Deputies (4 April 2012).
23 May 2012	Statement by the European Economic and Social Committee (EESC)
15 January 2013	First reading in the European Parliament (EP)
5 February 2013	Adoption by the EP and Council, publication in the Official Journal of the European Parliament, entry into force.

Options for Influencing the Political Process

Leading Directorate General:	DG Justice
Committees of the European Parliament:	Civil Liberties, Justice and Home Affairs (leading), rapporteur Jan Philipp Albrecht (Fraction Greens/EFA, D)
Committees of the German Bundestag:	Internal Affairs (leading)
Decision mode in the Council:	Qualified majority (approval by a majority of Member States and at least 255 out of 345 votes; Germany: 29 votes)

Formalities

Legal competence:	Art. 16 (2) TFEU (Data Protection), Art. 114 TFEU (Single Market)
Form of legislative competence:	Shared competence (Art. 4 (1), (2) TFEU)
Legislative procedure:	Art. 294 TFEU (ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

Harmonising data protection law and assigning EU-wide competence to a national authority tends to result in a reduction in effort and cost for the **companies** concerned **and to create a level playing field**.

Legal Assessment

Competency

Unproblematic. The legal basis is mainly the new EU data protection power (Art. 16 (2) TFEU).

Subsidiarity

A regulation at EU level makes sense when it concerns cross-border matters, especially as the regulation of the "placeless" medium of the internet can only succeed within a transnational framework. Where only national matters are affected, an EU-wide uniformed regulation is questionable. One argument in favour of an EU regulation is that otherwise, for very similar transactions, there would be two different data protection law regimes. It is in particular through the internet – the regulation of which is the main objective of the reform – that the relevance of crossing the border is evened out; there it is for both suppliers and users virtual.

Proportionality

The legal form of the regulation prevents EU data protection law from being implemented differently in the individual Member States. For the effective regulation of the internet this may be crucial, as otherwise there is the danger that companies might move to countries with the lowest requirements. On the other hand, full harmonisation also for domestic matters is not necessary and therefore disproportionate. However, the current Data Protection Directive as interpreted by the ECJ already brings about harmonisation to a large degree, thus amending the status quo seems more dramatic than it actually is.

Compatibility with EU Law

The design and the number of the powers conferred upon the Commission are not acceptable in terms of the division of power. **Decisions which are essential** for one branch of law **must be made by the European legislator itself** (cf. Art. 290 (1) TFEU). Moreover, the exact impact of the reform is hard to predict regarding actual practice in view of the numerous "gaps" within the regulation text.

Extending the regulation to include processors seated outside the EU is not questionable from a legal point of view. States – and also the EU – may regulate an issue, provided it has a sufficiently close material connection to its territory. The practice of international law and doctrine in general, as well as ECJ case law in particular, are generous in this respect (see last ECJ, C-366/10, Air Transport Association of America and others, paras. 110, 121 et sqq.). Linking, as provided, the regulation of such controllers to the data subject being resident in the EU – relevant in particular for internet use – will then no longer be problematic. Particularly unproblematic is extending the Regulation to cover controllers in the EU for cases in which the data are processed outside the EU. The actual enforceability of the EU data protection standards in all these cases is another question.

Clarification is needed when it comes to defining when exactly the data processing of a controller from outside the EU, particularly in internet matters, is "related" to offering goods or services to users seated in the EU. Similar difficulties in drawing distinctions can be found in the field of jurisdiction over consumer contracts (cf. ECJ, C-585/08 and others, Pammer).

The "right to data transfer" is mainly tailored to internet matters (e.g. social networks); however, in its scope it goes unnecessarily far beyond.

The rule that the consent of the data subject concerned does not legitimate the processing of data where a "significant imbalance" is given between the position of the controller and the data subject is not really concrete and therefore questionable. For instance, in the relationship between insurance companies and their clients it is not quite **clear whether there is such a "significant imbalance"**, or not. **In fact, often there will be no other legal basis for processing data related to health apart from a given consent** (cf. Art. 81, Art. 9 (2) lit. h), though processing this data is important for several insurances. Therefore, the provision should be revised and, at least, case examples be added, especially, because high fines are pending where no consent is given (Art. 79 (6) lit. a). The same holds true for the vague and inconsistent provision on designating a data protection officer in enterprises employing less than 250 employees (Art. 79 (6) lit. j); after all, the Regulation allows for substantiating legislation by the Commission itself (Art. 35 (11) in conjunction with Art. 86).

The rules concerning data protection of employees are rather cryptic: on the one hand, the Commission stresses its harmonisation aim, while on the other hand, the already existing harmonised rules in this field (cf. last ECJ, C-468/10 and others, ASNEF) are to be relaxed – however "within the limits of this Regulation" only – and the Commission even empowered to adopt delegated legal acts (Art. 82 (3)). **Hence,** in future, **national legislation in this field will face considerable legal uncertainty.**

Introducing class action gives cause for concern, in particular, because there are no specific requirements the bodies, organisations or associations eligible for class action have to match (apart from the rather unspecific objective to protect data and being duly registered in line with the law of a Member State).

Conclusion

Harmonising data protection law and assigning EU-wide competence to a national public authority reduces the costs of the companies affected and creates a level playing field. The design and the number of the powers conferred upon the Commission are not acceptable in terms of the division of powers. Decisions which are essential for one branch of law must be made by the European legislator itself. The rules regarding the invalidity of the consent are insufficiently concrete; moreover, here, too, the necessity to process data related to health should be taken into account. The rules regarding employees' data protection do not serve legal certainty.