On-going data protection reform (GDPR)

Main issues and stakeholders' views

1. Introduction

This note seeks to provide a brief overview on the on-going reform of the European Data Protection legal framework, focusing on the main innovations. Different stakeholders' perspectives and debates about main issues at stake are also reported.

2. The current regime

The current European data protection regime, under review, is represented mainly by Directive 95/46/EC (Data Protection Directive), which contains general principles on the *protection of individuals* with regard to the processing of personal data and on the *free movement of such data* as well as by other specific legislative instruments such as the e-Privacy Directive[1], concerning the processing of personal data and the protection of privacy in the *electronic communication sectors* and the Data Retention Directive[2].

Data processing by police and Law enforcement authorities in the context of police and criminal justice (former III pillar) are, for the time being, covered by the Council Framework Decision 2008 (which only applies to police and judicial data exchanged among Member States and EU authorities, not including domestic data) and by the national legislations of each Member States[3].

The legal basis for data protection, after the adoption of the Lisbon Treaty, is now provided by the TFEU (Article 16). Moreover, the Charter of fundamental Rights of the EU (2000) recognises to everyone the right to data protection (Article 8) as well as to privacy (Article 7): with the entry into force of the Lisbon Treaty in 2009 and the Charter acquiring the binding value of primary law, data protection is to be considered and treated as a fundamental right in EU, with the consequence, among others, that EU (secondary) law should be in line with its conditions. Recent ECJ rulings have underlined this principle[4].

2.1. Data Protection Directive

Directive 95/46/EC sets general principles as well as conditions/obligations for everyone who processes personal data (data controllers) as well as rights for data subjects. Exceptions to the general principles and rules are not missing.

---

[1] The e-Privacy directive has been modified by Directive 2009/136/EC. The Commission is committed to review again the ePrivacy Directive by 2016 with a focus on ensuring a high level of protection for data subjects and a level playing field for all market players (not only traditional telecoms companies).

[2] The Data Retention Directive has been declared invalid by the Court of Justice of the European Union on 8 April 2014 for the serious interference with private life and data protection that it would entail (Joined Cases C-293/12 and C-594/12 'Digital Rights Ireland'). More information on the Directive can be found here. See the publication commissioned by the GREENS Group on the retention directive after the judgement of the ECJ: http://www.greens-efa.eu/fileadmin/dam/Documents/Studies/Data/FB_MDC_Study_Data_Retention_Judgment_June_2014_FINAL_EXEC_SUMM.pdf.

[3] Beside these EU legal instruments, international acts apply, such as CoE Convention 108/1981, the European Convention on Human Rights (art 8 on privacy right), the OECD Guidelines (non-binding).

[4] See the ECJ Decisions, in the ' Google Spain' case (Case C-131/12 *Costeja*) on the right to delete personal data, or the Decision that invalided the Data Retention Directive (Joined Cases C-293/12 and C-594/12 ' Digital Rights Ireland').

First of all, protection rules apply when a person can be identified, directly or indirectly, by such data.
The main principles that can be inferred by from the directive (and that are not changed but strengthened in the proposed reform) are: **fairness and lawfulness of processing; purpose limitation** (data must be collected for specified, explicit and legitimate purposes); **data minimisation** (data must be adequate, relevant and not excessive in relation to the purpose); **accuracy of** data (data must be accurate and, where necessary, kept up to date); **storage limitation** (data should be kept in a form that permits identification of a person only as long as it is necessary for the purpose for which they were collected).
However, as said before, the aim of the directive is to allow a coherent free movement of data while protecting individual rights, therefore, data processing is not prohibited but subject to specific **conditions and grounds**, namely: subject' consent; compliance with a legal obligation; existence of a contract; vital interests of the data subjects; public interests; or legitimate interest of the controller or a third party that overrides the subject's privacy.[5]
Processing sensitive data (art 8) is allowed only under specific conditions.
Regarding the **scope** of the directive, it has a territorial limitation, according to the principle of establishment of the controller activities in the territory of the EU (or of the equipment, situated on the territory of a Member State). This is one of the main aspects changed with the reform (see below).
While the free flow of data is not discouraged, the Directive protects individuals to the extent that **transfer** of data outside EU/EEA is allowed only if the third country can ensure an adequate level of protection (art 25). This provision has recently been evoked by the **ECJ** in the case regarding the ' Safe Harbour' agreement with the U.S. (see below).

> According to Art 25, Directive 95/46/EC:
> (2)" the *adequacy* of the level of protection afforded by a third country shall *be assessed in the light of all the circumstances* surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, *the rules of law, both general and sectoral*, in force in the third country in question and the professional rules and security measures which

[5] Art 13 of the Directive establishes that Member States may adopt legislative measures to restrict the scope of the obligations and rights provided by the same Directive when it is necessary to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

are complied with in that country". (4) "Where the Commission finds [by adopting a Decision] that a third country does not ensure an adequate level of protection[...], Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question" . (5) "At the appropriate time, the Commission shall enter into *negotiations* with a view to remedying the situation resulting from the finding made pursuant to paragraph 4". (6) "The Commission may find, [by adopting a Decision] that a third country ensures an adequate level of protection [...] by reason *of its domestic law* or of *the international commitments* it has entered into, particularly upon conclusion of *the negotiations* referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals"

3. The Reform Package

The aim of the Directive 95/46/EC was *ensuring a functioning internal market and an effective protection of the fundamental right of individuals to data protection*[6]. The same objectives as well as its principles and grounds are still considered valid 20 years later, but the need to adapt data protection rules to the rapid technological developments and globalisation and to face new challenges have brought the EU legislators to reform the legal framework.

The three main institutions of the EU (European Parliament, the Council and the European Commission) are working since years[7] on the reform 'package', seeking to adopt a *comprehensive* legal framework able to cover data processing in the whole range of areas. The reform package, published by the EC in 2012, is constituted by two legal instruments[8]:

- A Proposal for a **General Regulation** 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*), as such, directly applicable in all Member States;
- A Proposal for a **Directive** on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - *Police and Criminal Justice DP Directive* (which needs to be transposed into national laws).

The aim of the reform package is to update and modernise the principles enshrined in the 1995 Data Protection Directive in order to guarantee the right of personal data protection in the future. The focus is on:

- reinforcing individuals' rights;
- strengthening the EU internal market; ensuring a high level of data protection in all areas, including police and criminal justice cooperation;

---

[6] EC, factsheets, Why do we need an EU data protection reform?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

[7] See EC COMMUNICATION *Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*, http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009.

[8] The reasons of the choice made for two separate legal instruments (i.e., a specific Directive for law enforcement (a Directive) are explained in the Explanatory Memorandum of the Regulation and of the Directive: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf as well as in the Impact Assessment accompanying the two documents.

- ensuring proper enforcement of the rules; and
- setting global data-protection standards.

The **European Parliament** adopted its first reading position on the reform on 12 March 2014. The LIBE Committee, responsible for the reform package, has produced in November 2013 two reports on the respective legal instruments, containing several amendments to the Commission original texts: the Albrecht Report (on the Regulation) and the Droutsas Report (on the Police Directive).
Some other EP Committees have expressed their Opinions on the reform, proposing ameliorations.
For instance, in the EMPL Opinion on the Regulation it was pointed out that:
Although a large volume of data processing in the EU relates to employment, little space in the Regulation is specifically devoted to employee data protection. Furthermore the level of abstraction of the Regulation often makes it difficult to interpret the rules in an employment context.
In the ITRE Opinion on the Regulation it was stressed that:
The proposed changes should help avoid excessive administrative burdens for enterprises, especially for those enterprises that have embedded privacy accountability, and guarantee a certain level of flexibility concerning some provisions of the Regulation, in particular those regarding the accountability mechanism and the notification to the supervisory authority.[...]
It is important to also place emphasis on the role of technical solutions such as privacy by design, pseudonymisation and anonymisation of data, prioritising the protection of sensitive data and targeted compliance.
The IMCO Opinion on the Regulation underlined the Internal Market dimension:
The proposal has a high potential for enhancing the internal market and creating a level playing field for all businesses active in the EU. Key elements include:
- the shift of the legislative instrument (from directive to regulation);
- the 'one-stop shop' principle regarding the competent supervisory authority in cross-border cases;
-the marketplace principle (which makes EU data protection standards also applicable to businesses based outside the EU, if they are active within the EU);
- the general principle of accountability (which replaces the obligation of data controllers or processors to make a general notification about their processing to their national regulator).
While the JURI Opinion on the Regulation stressed, among other issues
the general principle of the responsibility of the controller. The proposal for a regulation reinforces the obligations of controllers, thereby enabling the rights of the individual concerned to be effectively exercised. However, more measures are needed if this general principle of responsibility is to be established explicitly. The 'right to be forgotten' should also be strengthened.

See also the JURI Opinion on the Directive (i.e. on the Proposal for the Police and Criminal Justice Directive) of the 16.04.2013.

On 15 June 2015 **the Council** of the European Union reached a general approach on the draft Regulation and negotiations with the EP seem moving forwards quite rapidly (*trilogues*). The adoption of **the Directive on data processing in the police and criminal Justice cooperation** may take longer than that of the General Regulation; however, the adoption of the whole package by the end of 2015 is urged by all sides and recently (9 October 2015) the Council had also reached an agreement on the general approach of the proposed Directive for new data protection rules in law enforcement: negotiations with the EP, in a spirit of compromise, can now also include this Directive.

The **European Economic and Social Committee** expressed its Opinion on the Regulation already on 23 May 2012, in which while regretting the fact that the stated principles of the right to protection of personal data are qualified by an excessive number of exceptions and restrictions, it welcomed the general direction taken by the Commission:
In the new context of the digital economy, the Committee shares the Commission's opinion that, "individuals have the right to enjoy effective control over their personal information" and considers that this right should be extended to cover the various purposes for which individual profiles are drawn up on the basis of data collected by numerous (legal and sometimes illegal) methods and its processing[...]
The EESC believes that search engines, the majority of whose revenue comes from targeted advertising thanks to their collection of personal data concerning the visitors to their sites, or indeed the profiling of those visitors, should come expressis verbis within the scope of the regulation. The same should go for the sites of servers providing storage space and, in some cases, cloud computing software, that can collect data on users for commercial ends.

The **European Data Protection Supervisor** (EDPS - an independent supervisory authority), has proactively intervened during the legislative *process* of the reform providing his Opinions and (recently) recommendations, urging the co-legislators to achieve with the reform package "a consistently **high level of protection** across all sectors and to retain the individual and **human dignity** at the heart of the EU data protection reform, shielding individuals from harm and **empowering them** to take control over their personal information in cyberspace. **Trust** is a necessary precondition for innovative products and services that rely on the processing of personal data and the GDPR needs to be a blueprint for an ethical approach."[9] The EDPS stressed in particular the fact that existing principles set down in the Charter should be applied consistently, dynamically and innovatively so that they are effective for the citizen in practice.
His recommendations, which call for a ' package approach', are shaped by three main concerns:

- a better deal for citizens
- rules which will work in practice
- rules that will last a generation.

The relevance of the adoption of the data protection reform package for achieving a Single Digital Market, has been recently stressed by the **European Commission** in its COM(2015) 192 final: *Businesses and consumers still do not feel confident enough to adopt cross-border cloud services for storing or processing data, because of concerns relating to security, compliance with fundamental rights and data protection more generally. The adoption of the data protection reform package will ensure that the processing of personal data is governed by uniform, up-to-date rules throughout the Union*[10]. Pres. Junker also stressed the need to safeguard consumers' fundamental rights to privacy and personal data protection while also encouraging innovation.

3.1. Scope, objectives and main innovations

Strengthen privacy and data protection is considered instrumental also to innovation and development. As many European citizens seem to be unconfident towards online companies or

[9] See A welcome step towards the reform of Data Protection rules in Europe / EDPS Press Release, October 2015.
[10] To be noted that among the future initiatives of the EC, there is a European Free Flow of Data initiative to address existing restrictions on the free movement of data for reasons *other than* the protection of personal data within the EU and unjustified restrictions on the location of data for storage or processing purposes (including issues of ownership, interoperability, usability and access to data). It will encourage access to public data to help drive innovation. Moreover, the Commission will launch a European Cloud initiative including cloud services certification, contracts, switching of cloud services providers and a research open science cloud, see COM(2015) 192 final, p.15.

governments as regards their data[11], fostering **trust** in new online services and strengthening the individual rights (including with appropriate remedy mechanisms) are among the objectives of the reform. Moreover there are still divergences in rules across Member States which create barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement.
For this reasons, several changes have been introduced by the reform with the aim to enhance the implementation of data protection rules, such as:
- *A single set of rules on data protection, valid across the EU*. Regulation has direct application within member states, without the need for implementing national laws (proposed Police Directive has not);
- a *wider scope*: as regards its territorial application, the Regulation introduced (beside of the already existing *establishment* criterion of the Directive 95/46/EC) a 'functional' criterion, so that it will be applicable:
a) *to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union*
b) *to the processing of personal data of data subjects residing in the Union by a controller not established in the Union* [e.g. **non-EU companies]** ***that offer goods or services in the EU or monitor the online behaviour of citizens***.
Moreover, art 40 and following sets a series of conditions for any transfers of personal data to third countries or international organisations, including onward transfers.

Other **relevant changes** introduced with the General Regulation include:

- *Explicit consent*: Whenever consent is required for data processing, it will have to be given explicitly, rather than be assumed.
- *Transparency*.
- *Data Portability*: easier access to one's own data and the right of data portability, i.e. easier transfer of personal data from one service provider to another.
- A '*right to be forgotten'* will help people better manage data-protection risks online. When they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
- *Data breaches notification*. Companies and organisations will have to notify serious data breaches without undue delay, where feasible within 24 hours.
- *One-stop shop.* If a company is established in several Member States it will only have to deal with a single national data protection authority – in the EU country where they have their main establishment.
- *Remedies*. Individuals will have the right to refer all cases to their home national data protection authority, even when their personal data is processed outside their home country.
- *Accountability*. Increased responsibility and accountability for those processing personal data.
- *Designation of the data protection officer* : [12]

[11] See the Special Eurobarometer 359,Attitudes on Data Protection and Electronic Identity in the European Union, June 2011

[12] Art 35: *Designation of the data protection officer*

> *1. The controller and the processor shall designate a data protection officer in any case*
>
> *where:*
>
> *(a) the processing is carried out by a public authority or body; or*
>
> *(b) the processing is carried out by an enterprise employing 250 persons or more;*

– *Less bureaucracy*. Unnecessary administrative burdens such as notification requirements for companies processing personal data will be removed.

Moreover, technology developers and users will have to comply with the principles of *Privacy/Data Protection by Design and by Default* (i.e. 'to embody' data protection requirements into technology, product or service since the beginning). In particular, the EP urges that the **effective protection** of rights is listed as one of the principles of the reform: in the field of data protection it is necessary to ensure that procedural rights are built into the system (the so-called 'privacy by design'). An example would be a social network that makes it easy to complain that the user's privacy has been violated[13].

The grounds for a lawful data processing set out by the reform are based on Directive 95/46/EC: consent, existing contract, compliance with a legal obligation, vital interest of data subject; public interest or **legitimate interest of the controller**. The latter rule is particularly important for the private sector, in the absence of consent or a contract (in Google Spain case, mentioned above in fn 4, the ECJ ruled that the privacy interests of those named in search results prevail over Google's interests)[14].

4. Data transfer to US and the recent Court of Justice' Decision ('Safe Harbour')

Following a complaint against Facebook by an Austrian citizen and privacy activist, Max Schrems, the European Court of Justice ruled on 6 October that the Commission's "adequacy Decision" (on U.S. level of protection to data transferred from EU to U.S. and adopted pursuant to art 25 Directive 95/46, mentioned before) was invalid, since the "Safe Harbour" scheme does not afford the adequate protection required by EU law. Schrems brought the case arguing that Edward Snowden's revelations of the US National Security Agency's PRISM data collection programme, under which EU citizens' data held by US companies was transferred to US intelligence companies, calls into question the adequacy of the data protection afforded by the Safe Harbour agreement. Transferring data by Facebook (as by other companies) under the "Safe Harbour" agreement was in fact declared by the Court unsafe. The case is being widely debated in the EP in these days.

The European Parliament has repeatedly called for the suspension of Safe Harbour, most recently in its 2014 resolution on the surveillance programme carried out by the NSA and by surveillance bodies in various member states. In this resolution the Parliament considered in particular the impact of these programmes on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. The resolution concluded a six-month Parliament inquiry on electronic mass surveillance of EU citizens, following the revelations made in June 2013 on alleged spying by the US and some EU countries. In its resolution, Parliament called for the suspension of the Safe

---

or

(c) the core activities of the controller or the processor consist of processing

operations which, by virtue of their nature, their scope and/or their purposes,

require regular and systematic monitoring of data subjects.

[13] See S. Peers, Basic data protection principles in the proposed Data Protection Regulation: Back to the Future? http://eulawanalysis.blogspot.be/, of the 9/03/2015.

[14] On this regard, the institutions had initially different opinion on what happens if the **purpose** of data processing is changed. The Commission proposed that changing the purpose should be acceptable on any of the grounds for the initial processing of the data, except for the legitimate interests of the controller. The Council wanted to allow a change of purpose for any of the grounds for the initial processing, including the legitimate interests of the controller; while the EP did not want to provide expressly for any incompatible processing at all. See S. Peers, Basic data protection principles in the proposed Data Protection Regulation: Back to the Future? http://eulawanalysis.blogspot.be/, of the 9/03/2015.

Harbour privacy principles (voluntary data protection standards for non-EU companies transferring EU citizens' personal data to the US) and of the Terrorist Finance Tracking Programme.

5. Reactions

Below are reported some reactions to both the Data Protection reform package and to the recent ECJ ruling on Safe Harbour.

EP Reactions to the ECJ ruling on Safe Harbour Decision
EP Plenary Session;
Parliamentary question (8/10/2015)
LIBE position Statement of Pres. Moraes (call on the EC to act immediately);

Political Groups
EPP - Position Paper on Data Protection Reform, 02/07/2015
S&D - Position paper, 2013; Statement after safe harbour ruling, 6.10.2015
ALDE - Press release 25.6.2015
GREEN - on the reform package: State of Play in 10 main issues; Press release after the Safe Harbour ruling: 8.10.2015 & 6.10.2015 ; Privacy campaign
GUE - Privacy and data protection rights in a digital era
ECR - Position Paper on digital single market - see p.14-15 for data protection
ENF - It seems that the group has not taken any position on the issue.

Stakeholders
Targeted consultations on the data protection reform were conducted with key stakeholders (Member State authorities and with private sector stakeholders, as well as privacy, data protection and consumers' organisations), the summary of which are collected here [15]
Among them:
Letter from different **NGOs** to President Juncker, 21.4.2015 and response from Head of Cabinet of Vice President Timmermans, 17.7.2015, https://edri.org/files/eudatap/Re_EC_EDRi-GDPR.pdf
Federation of European Direct and Interactive Marketing, position paper, 2015
Direct Marketing Association position (Public Consultation), 2009
Orgalime position paper, (voice of the EU engineering industry)
EuroISPA position (Public Consultation), 2009
E-commerce Europe position paper on privacy and transparency, 2014;
Microsoft position (Public Consultation), 2009;
Yahoo! position (Public Consultation), 2009;
European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry, position paper, 2014
World Federation of Advertisers, policy paper 2012

Google's concerns on the right to be forgotten (2012)
CPDP conference, panel of privacy innovators (2015)
BBC news: How worried is Silicon Valley about Safe Harbour (7/10/2015)

Further reading
-on the Reform: EP policy briefings

[15] http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm

- on the Safe Harbour Court ruling (S. Peers blog), Financial Times; La libre.be