INTO THE UNKNOWN – THE PROPOSED EU GENERAL DATA PROTECTION REGULATION AND ITS POTENTIAL EFFECT ON TRANSBORDER DATA FLOWS

Cecilia Alvarez[1], John Bowman[2], Natascha Gerlach[3] [4]

Data Protection has a long standing tradition in many European countries, with a right to one's own image existing in Germany and France as early as the beginning of the last[5] century, and the first data protection laws being introduced in the 1970s[6]. The OECD issued its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980[7], followed by Convention 108 of the Council of Europe[8] in 1981 regarding the protection of individual personal rights in connection with automatic data processing[9].

Within the EU, Article 8 of the Charter of Fundamental Rights recognized an "autonomous right to the protection of personal data" in 2000 for every individual in the EU.[10]

The centerpiece of current European Data Protection legislation is undoubtedly Directive 95/46/EC[11] which in 1995 was intended to provide the structure for the protection of fundamental rights and freedoms of individuals in the member countries while ensuring at the same time the free flow of information in support of the internal market.[12]

As a legal instrument under EU law, a Directive requires EU Member States to achieve a particular result without dictating the means of achieving that result. When adopted,

---

1 Cecilia Alvarez is the European Data Protection Officer at Pfizer

2 John Bowman is a Senior Principle at Promontory Financial Group UK

3 Natascha Gerlach is the Managing Attorney for EU Litigation Operations at Cleary Gottlieb Steen and Hamilton

4 Marta Janek, Maci-Brooke Smith, and Susan N. Hammond contributed to this article

5 Para 22, 23 Kunsturhebergesetz KunstUrhG dated January 9, 1907

6 German Federal State of Hessen, 1970, Austria, Denmark, France, Luxembourg, Norway, Sweden

7 http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

8 Not to be confused with the Council of the European Union. The Council of Europe is an independent body, not controlled by the European Union: http://www.coe.int/en/

9 http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

10 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, p. 4

11 Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

12 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, p. 2

Directives give Member States a timetable for the implementation of measures that will achieve the intended outcome.

The Commission published several reports on its monitoring of the implementation of the Directive by the Member States[13], which intended to ensure proper implementation and harmonisation throughout the reach of the Directive, as well as ensuring that it remains appropriate for embracing the development of new technologies[14].

With the ever increasing speed of technological advances, the Commission finally saw the need to take a closer look at the existing legal framework in 2009 and started a series of consultations and studies with an eye toward several key points[15]:

- The impact of new technologies
- The consistent lack of sufficient harmonization between Member States
- Globalisation and international data transfers
- Effective enforcement
- Less fragmentation of instruments

The Lisbon Treaty[16] of 2009 and, in particular, Article 16 of the Treaty on the Functioning of the European Union (TFEU) finally also cemented the principle of data protection for individuals in the context of the European Union and provided a direct basis for the adoption of rules to implement such protection[17]. Article 8 of the EU Charter of Fundamental Rights established an autonomous right to the protection of personal data, and Article 16 TFEU (ex Article 286 TEC) creates the means for the adoption of rules to protect those rights.

---

[13] First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final, of 15.5.2003; http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[14] COM(2007)87 final of 7.3.2007

[15] http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, p. 3 ff

[16] The Treaty of Lisbon Treaty was signed by EU Member States on 13 December 2007 and entered into force on 1 December 2009. It amends the Maastricht treaty from 1993 and the Treaty of Rome from 1958, introducing the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU).

[17] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT

On January 25, 2012, with the words "Ladies and Gentleman, we have done it", the then EU Justice Commissioner Viviane Reding introduced a reform package which included a legislative proposal for a General Data Protection Regulation[18], not a Directive as before.

This article will provide a brief overview over the impact of a regulation vs. a Directive and explain the legislative process that is required for the current proposal of Regulation to become a law. Finally, the article will analyse the key issues addressed to date by the three institutions with a particularly impact on transborder data flows, based on an overview over the developments to date.

Regulation vs. Directive

Article 288 of the Treaty on the Functioning of the European Union (TFEU) provides definitions for the legal instruments of directive and regulation.[19] The most significant difference between them is their applicability. While a directive does not have to be addressed to all Member States and is binding only as to the end to be achieved while leaving some choice as to form and method to the Member States,[20] regulations are legally binding in their entirety and directly applicable in all Member States. Regulations do not need to be transposed into national law by each Member State. Member States are also under a duty not to obstruct the direct applicability inherent in regulations.[21]

Another significant difference between regulations and directives is how they take effect. Regulations have direct effect, which means that individuals can rely on their provisions in national courts. Directives have vertical direct effect only, which means that individuals can rely on them in actions against the state. [22]

For the Commission, the legal instrument of a regulation was the means to "*reduce legal fragmentation and provide greater legal certainty by introducing a harmonized set of core*

---

[18] http://europa.eu/rapid/press-release_IP-12-46_en.htm

[19] According to Article 288 TFEU "a regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States" and "a directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."

[20] Directives have to be transposed into national law within the transposition period defined in the directive, usually eighteen or twenty four months after publication; see also Craig, P, de Burca, G, *EU Law: Text, Cases and Materials*, Oxford University Press, Oxford, p.106

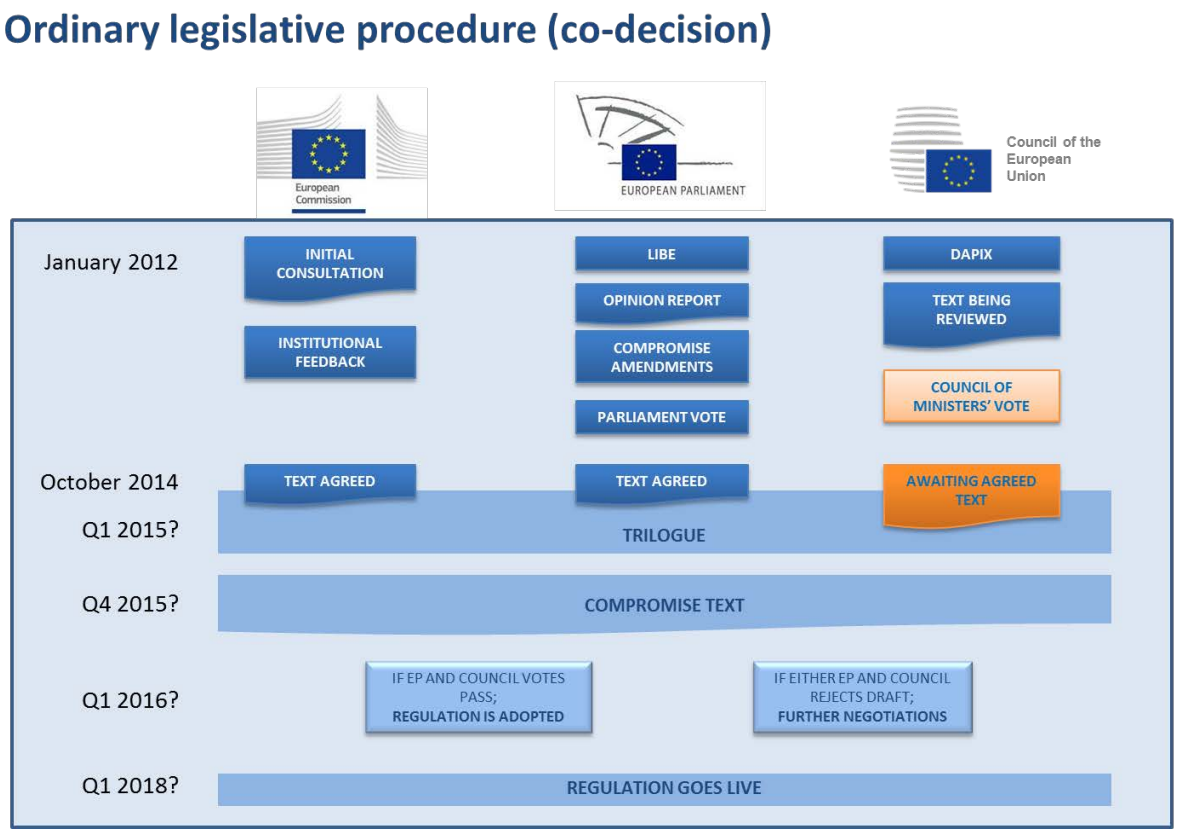
[21] Case 34/73 *Variola v Amministrazione delle Finanze*, para 10

[22] Craig, P, de Burca, G, *EU Law: Text, Cases and Materials*, Oxford University Press, Oxford, p.106

rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market".[23]

Legal process until the proposal of Regulation becomes law

Since the Lisbon Treaty, the majority of laws are passed under the so called "ordinary legislative procedure" in accordance with the procedure laid out Article 294 TFEU. This is also the case for the General Data Protection Regulation. In the ordinary legislative procedure (co-decision) the European Parliament and the Council of the European Union adopt a new Directive or Regulation jointly, after a proposal by the Commission.[24] The diagram below demonstrates this process as it applies to the proposed Regulation and the estimated timings:



The Parliament has the first opportunity to consider the proposal in a first reading and then sends its position to the Council of the European Union. The Council in turn can either

---

[23] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of personal data and on the free movement of such data (General Data Protection Regulation)*, p.5.

[24] Art. 289 (1) TFEU

approve the Parliament's version or adopt its own which would then go back to the Parliament.[25]

The proposed General Data Protection Regulation was submitted by the Commission to the European Parliament and the Council.[26] In Parliament, the President referred the proposal to the Committee on Civil Liberties, Justice and Home Affairs (LIBE),[27] which appointed Jan Philipp Albrecht as rapporteur.[28] The function of the rapporteur is essentially to guide the proposal through the stages, advising LIBE and Parliament as a whole, [29] as well as drafting a report to LIBE on the proposal, which in this case has become known as "The Albrecht Report".[30]

On March 12, 2014, the Parliament voted to formally adopt the proposed legislation.[31] This concluded Parliament's first reading. The proposal moved to the Council of European Union for its first reading, which is still ongoing.

The Council has assigned the proposal to DAPIX (Working Party on Information Exchange and Data Protection), a working group of the Council's Justice and Home Affairs Council (JHA). A revised version of the proposal was published under the Lithuanian Presidency[32], a series of notes on various topic like data transfers, one-stop shop, or data portability were published under the Greek Presidency of the Council[33] . Under the Italian Presidency, the

---

[25] See Art. 294 TFEU for the full procedure

[26] http://www.europarl.europa.eu/aboutparliament/en/0081f4b3c7/Law-making-procedures-in-detail.html

[27] http://www.betterregulation.com/ie/hot-topic/data-protection

[28] *See id.*

[29] http://www.europarl.europa.eu/aboutparliament/en/0081f4b3c7/Law-making-procedures-in-detail.html

[30] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

[31] *See id.*

[32] The presidency of the Council of the European Union rotates every six months between Members States;.http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F13%2Fst17%2Fst17831.en13.pdf

[33]http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%205879%202014%20INIT;
http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%205345%202014%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F14%2Fst05%2Fst05345.en14.pdf

Council published a further revised version of the Regulation in December 2014.[34] Although the Council seems to be some way from a final vote, and there is no time limit for this first reading, progress is being made.[35] The Latvian presidency of the Council, which took over in January 2015, stated that making progress on the data protection package, towards achieving a negotiating mandate for the Council, will be one of the Presidency's first priorities.[36]

Where we are now

In March 2015 the Council agreed its version of the one-stop shop and ministers committed to agreeing the remainder of the Council position at the June meeting of the Justice and Home Affairs Council.[37]

When the Council does agree a general approach, the Parliament and the Council will need to work out how much ground they can concede in the informal trilogue discussions while remaining within their respective negotiating mandates. Around the table will be a senior official from the Commission who will mediate discussions, the rapporteur from the LIBE Committee, and the chair of the DAPIX working group from the Council Presidency.

In June 2015, the Council would be represented in trilogue by the Latvian Presidency until the end of June, with Luxembourg stepping in from July to December 2015. If the discussions continue beyond, the Netherlands will represent the Council in the first half of 2016. However, there is some political momentum for agreement to be reached before the end of 2015, particularly as the European Council[38] had set the end of 2015 as the deadline for final agreement of the Regulation at a meeting in October 2013.[39]

During the course of the trilogue negotiations, the Parliament and the Council of the European Union will aim to reach a first reading agreement in order to avoid a second or

---

34 http://data.consilium.europa.eu/doc/document/ST-15395-2014-INIT/en/pdf

35 *See id.*

36 http://www.mfa.gov.lv/en/brussels/priorities; http://www.statewatch.org/news/2015/apr/eu-council-dp-reg-4column-2015.pdf

37 http://www.statewatch.org/news/2015/apr/eu-council-dp-reg-4column-2015.pdf

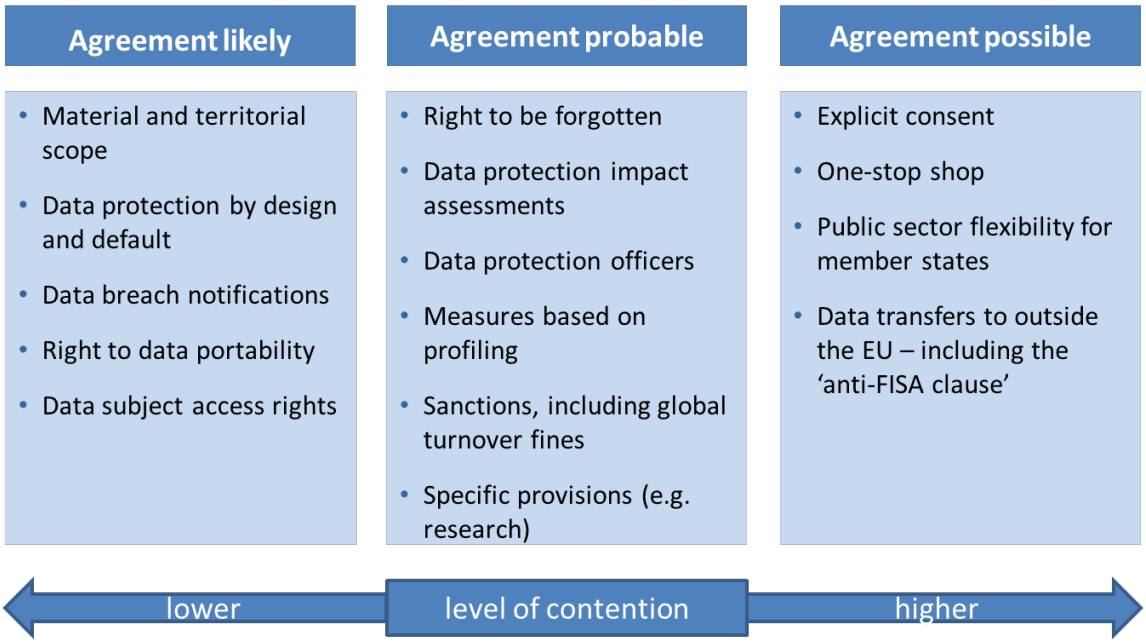
38 This body consists of the EU member state heads of government; it is distinct from the Council of the European Union.

39 https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

third reading of the text which would activate further legislative procedures, negotiations and rounds of voting.

However, the Parliament and Council will enter trilogue from different positions and how easily these can be resolved depends on how entrenched the views of these institutions remain during the course of discussions. Examples of topics which may prove more difficult to agree on include; explicit consent, the one-stop shop, and the so-called "anti-FISA clause".

Possible trilogue compromises



Whatever representatives of the Parliament and Council can agree on though, the final text is likely to cut across one of the key claimed advantages of the Commission's proposals, that is the introduction of harmonized rules and a reduction in legal fragmentation across EU borders through the consistent interpretation and enforcement of the new rules.

If the Council Presidency can successfully argue for flexibility in trilogue, in particular around the local competence of regulators, then the Commission's original vision of a fully harmonized framework in accordance with EU single market principles may end up being diluted.

Key issues which may impact transborder data flows

With the above in mind, certain key issues of the proposed Regulation will impact transborder data flows, in particular, within the context of discovery or law enforcement proceedings.

1. Territorial scope

The territorial scope of the EU data protection regulations will be broader than the one set forth by the Directive and will more easily apply to non-EU data controllers. Indeed, the Regulation is intended to apply:

(i) the processing of personal data in the context of the activities of an establishment in the EU not only of a controller but also of a processor; or

(ii) the processing of personal data of data subjects residing in the UE by a controller not established in the EU, where the processing activities are related to:

(a) the offering of goods or services to such data subjects in the EU; or

(b) the monitoring of their behavior.

2. Consent

Both the Commission and the Parliament consider that the data subject's consent must be "explicit" in all events. However, the Council limits the "explicit" nature of the consent to instances, where the processing (i) refers to sensitive data; (ii) is carried out for profiling purposes; (iii) consists of transfers outside the EEA to non-adequate recipients.

The three institutions agree, that consent should not be regarded as freely-given if the data subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment. The same would apply if there is a clear imbalance between the data controller and the data subjects. According to the Commission and the Parliament, this imbalance always exists when the data controllers are employers vis-à-vis their employees (or public authorities).

3. International transfers

The regime set forth in the Directive (i.e., existence of an adequacy decision issued by the Commission, adoption of appropriate safeguards and existence of derogations) is kept "as is" with some relevant changes:

(i) <u>Adequacy decisions</u>

The former adequacy decisions adopted by the European Commission on the basis of Article 25(6) of the Directive (which was the legal basis of the Safe Harbor Decision, among others) shall be in force, until amended, replaced or repealed by a new Commission Decision. The Parliament did not change this principle but introduced a maximum term of 5 years in case of inactivity of the Commission.

(ii) Appropriate safeguards (applicable to both the data controllers and, for the first time, also to the data processors)

These are summarized in the chart below (green where safeguards have been considered by the institution):

Appropriate safeguards		**Commission**	**Parliament**	**Council**
No [further/specific] Data Protection Authority (DPA) authorisation	Binding/enforceable instrument between public authorities			
	BCR (Binding Corporate Rules)	[for controllers and processors]	[for controllers and "external subcontractors of the controller's group of undertakings"]	[for controllers/processors and Group of enterprises engaged in a joint economic activity]
	Commission model clauses (*)			
	DPA model clauses			
	Certifications		European Data Protection Seal	Approved code of conduct + data exporter commitments
				Approved certification mechanism
DPA authorisation	Clauses between exporter and importer			

(*) The Commission and the Parliament have adopted the same rule as the one followed for the former adequacy decisions. However, the Council remains silent in this respect.

(iii) Derogations

The three institutions agree on keeping the same derogations as those listed in the Directive: risk-informed consent (now explicit); the (pre) contractual relationship with the data subject or data subject's interest; the public interest (under EU law or the controller's Member State law); legal claims; vital interest and the public registry source.

In addition, the Commission (for both controllers and processors) and the Council (only for controllers) have included the "legitimate interest" ground among the derogations only for transfers that are not massive or frequent.

In this respect, it must be noted that the Council also provides that "*controllers that are part of a group of undertakings or institution affiliated to a central body may have a legitimate interest to transmit personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country (…) remain unaffected*". However, by their own nature, these transfers should actually be massive and frequent.

(iv) Anti-FISA provision

The so-called anti-FISA provision has only been included in the Parliament text. It requires both data controllers and data processors to notify DPAs about requests to disclose personal data to courts or regulatory authorities in countries outside of the EU, and to obtain formal approval of DPAs before turning over European data. The text also provides that "*any legislation which provides for extra-territorial access to personal data processed in the Union without authorization under Union or Member State law should be considered as an indication of a lack of adequacy*" (Recital 82).

4. One-stop-shop

The rationale for the one-stop-shop approach is to have a single DPA, such as the DPA of the "main establishment" of organizations with more than one establishment in the EU, competent for all of its data processing activities in the EU.

Contrary to the initial Commission proposal that provided for a true one-stop-shop approach, the Parliament text created a "lead DPA" system. The lead DPA would be the sole authority empowered to take legal decisions with regard to a company, but would have complex cooperation obligations with regard other DPAs. Furthermore, individuals could lodge a complaint before the DPA of their home jurisdiction, and the lead DPA would be required to coordinate its work with that DPA.

According to the Council, the one-stop-shop mechanism should only play a role in cross-border cases and will provide for cooperation and joint-decision making between several DPAs concerned (in addition, excludes the processing activities carried out by the public sector from this mechanism).

5. Legitimate interests

The legitimate interest (and associated balance test):

(i) Is one of the legal grounds for non-sensitive data processing activities, only with respect to the controller (Commission) or also with respect to a third party as originally set forth in the Directive (Parliament and Council); provided that it meets the expectations of the data subject based on his/her relationship with the controller (only the Parliament).

(ii) Must be disclosed to the data subject as a general rule and described in the prescribed documentation.

(iii) Is one of the derogations to justify an international transfer of both a data controller and a data processor if not massive or frequent (Commission and Council).

6. Legal claims

If necessary for the establishment, exercise or defense of legal claims:

(i) the processing of sensitive data or the transfer for non "adequate" data importers shall be legitimate; and

(ii) (specified only in the Council text) the (new) right to be forgotten and the right to object shall not apply.

7. Sanctions

All DPA of the EU Member States will have wide powers to investigate and enforce. In particular, they will be empowered to fine companies that violate EU data protection rules. This can lead to penalties of up to €1 million (Commission) or €100 million (Parliament) up to 2% (Commission) or 5% (Parliament) of the global annual turnover of a company. The Council has not yet proposed a maximum threshold in terms of fixed amount or percentage of the turnover.

Closing remarks

It is more than three years since the European Commission proposed a comprehensive data protection reform. For the Regulation to become a law, the Commission, the Parliament and the Council must reach an agreement. While the European Parliament has approved its significantly amended version in March 2014, and the Council has reached significant "partial general approaches" on key aspects of the proposal, the Council's final text is still pending and not expected to be approved before this summer. If this is the case, the Regulation might go live in 2017 or 2018. However, regardless of the timing, it is only a question of "when" not "if" and it is clear, that the reform will have an impact on transborder data flows and in particular, transfers out of the EU/EEA. Where discovery or enforcement actions are involved, close attention will have to be paid to the changes in territorial scope, the amount of the sanctions, the role to be played by consent, the legitimate interest and the f legal claims derogations, as well as to whether or not an anti-FISA clause will be included in the international transfers regime. Whether or not the new Regulation will simplify the process as intended remains to be seen. It seems certain that a period of uncertainty lies ahead where guidance will be required from the DPAs and the equivalent of the Article 29 Working Party on to how to integrate existing case law and prior guidance on Directive 95/46 clauses into the new regime.