DATA PROTECTION TODAY: CHALLENGES AND PERSPECTIVES

Eleonora Bassi (Nexa Center)

On January, 25th 2012 The European Commission presented his official Proposal for

– a **Regulation** (replacing Directive 95/46/EC) setting out a general EU framework for data protection

– a **Directive** (replacing Framework Decision 2008/977/JHA) setting out rules on the protection of personal data processed for the purposes of **prevention, detection, investigation or prosecution of criminal offences and related judicial activities**

- **Opinion of the EDPS on the data protection reform package (7/3/2012)**
- **Art. 29 Working Party, Opinion 01/2012 on the data protection reform proposals, wp191 (23/3/2012)**

The Regulation has 3 Objectives:

Strengthen the right of individuals to data protection

Enhancing a Digital Single Market

Enforcing data protection in a globalized world

Principles:

Article 5 sets out the principles governing the processing of personal data, which correspond to those referred in Article 6 of Directive 95/46/EC. Among the new items are added:

the **principle of transparency** (→ Art. 11),

the **clarification of the principle of data minimization** and

the introduction of a **general responsibility of the controller**.

Article 6: **Lawfulness of processing**

Art. 7 **Conditions for consent** , Art. 8 **Processing of personal data concerning children**

Rights of the Data Subjects

Duty of transparent information and communication (Art. 11)
Information to the data subject (Art. 14)
Right of access for the data subject (Art. 15)
Right to rectification (Art. 16)
Right to be forgotten and to erasure (Art. 17)
Right to data portability (Art. 18)
Right to object (Art. 19)

Article 20 introduces **Measures based on profiling.**

Restrictions (1)

Restriction to:

Art. 5 (a): “processed lawfully, fairly and in a transparent manner in relation to the data subject”

Art. 5 (e) “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”

Artt. 11-20: Data Subject’s Rights

Art. 32: Communication of a personal data breach to the data subject

Restrictions (2)

Art. 21 (1): Union or Member State law **may restrict by way of a legislative measure** the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

(a) **public security**

(b) the **prevention, investigation, detection and prosecution of criminal offences**

(c) other **public interests of the Union or of a Member State**, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity

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

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

(f) the **protection of the data subject** or the **rights and freedoms of others**

Accountability

- **Responsability of the controller** (Art. 22)
- **Processor:** (Art. 26(2, 4)) The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller (…) If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers.
- **Data Protection by Design and by Default** (Art. 23)
- **Duty of Documentation** (Art. 28)
- **Duty of Co-operation with the supervisory authority** (Art. 29)
- **Data Breach Notification to the supervisory authority** (Art. 31), (→Article 4(3) of the e-privacy Directive 2002/58/EC)
- **Communication of a personal data breach to the data subject** (Art. 32)

(The Commission shall be empowered to adopt delegated acts)

Accountability and Transparency: the DPIA

Art. 33: **Data protection impact assessment**

1. Where processing operations present **specific risks** to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the **controller or the processor** acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…)
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.(…)
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities. (…)

Accountability and Standardization: the DPO

→ Directive 95/46/EC, Art. 18 (2)

Article 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; 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.

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body. (…)

Standardization

Codes of Conduct (Art. 38)

Certification (Art. 39)

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.
2. The Commission shall be empowered to adopt delegated acts (…) for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms (…), including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.
3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. (…)

Territorial scope:

→Art. 3 (1,2):

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

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

(b) the monitoring of their behaviour.

→ Art. 25(1): In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

Transfers to a Third Country

Article 41 states the criteria, conditions and procedures for the adoption of a **decision of the adequacy of the Commission**. The criteria should take into account the Commission to assess whether the level of protection is or less adequate expressly include the **state of law**, **judicial review** and an **independent control**. The article confirms that the Commission can now explicitly evaluate the level of protection offered by an area or treatment area within a third.

Article 42: **Transfers by way of appropriate safeguards**

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

safeguards:

(a) **binding corporate rules** (…); or

(b) **standard data protection clauses** adopted by the Commission. (…); or (*sub* c) by a supervisory authority in accordance with the consistency mechanism (…); or

(d) **contractual clauses** between the controller or processor and the recipient of the data authorised by a supervisory authority (…).

Delegated and implementing acts (1)

Art. 290 TFEU
Artt. 86-87, Proposed Regulation
Rec. 129, Proposed Regulation

The Commission shall adopt delegated acts for:

- **lawfulness** of processing
- specifying the criteria and conditions in relation to the **consent of a child**
- processing of **special categories of data**
- specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject
- criteria and requirements for the **information** to the data subject and in relation to the right of **access**
- the **right to be forgotten and to erasure**
- measures based on **profiling**
- criteria and requirements in relation to the **responsibility of the controller**
- **data protection by design and by default**
- **processor**

Delegated and implementing acts (2)

…for:

- criteria and requirements for the **documentation** and the **security** of processing;
- criteria and requirements for establishing a **personal data breach** and for its **notification** to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject;
- the criteria and conditions for processing operations requiring a **DPIA**;
- the criteria and requirements for determining a high degree of specific risks which require **prior consultation**;
- designation and tasks of the **DPO**;
- **codes of conduct**;
- criteria and requirements for **certification** mechanisms;
- criteria and requirements for transfers by way of **binding corporate rules**;
- **transfer derogations**;
- **administrative sanctions**;
- **processing for health purposes**;
- processing in the **employment** context and processing for **historical, statistical and scientific research** purposes.

Delegated and implementing acts (3)

Article 86: ***Exercise of the delegation***

The delegation of power (…) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation (…)

may be revoked at any time by the European Parliament or by the Council.

A delegated act adopted (…) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

DPAs

Article 51 introduces the '**one-stop shop**'.

Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors. (Rec. 97)

Co-operation:

Mutual assistance (Art. 55), **Joint operations of DPAs** (Art. 56)

Consistency Mechanism (1)

Article 58: ***Opinion by the European Data Protection Board***

1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:

(a) relates to processing activities which are related to **the offering of goods or services to data subjects in several Member States**, or to the **monitoring of their behaviour**; or

(b) may substantially affect the free **movement of personal data within the Union**; or

(c) aims at adopting a list of the processing operations **subject to prior consultation** pursuant to Article 34(5); or

(d) aims to determine **standard data protection clauses** referred to in point (c) of Article 42(2); or

(e) aims to authorise **contractual clauses** referred to in point (d) of Article 42(2); or

(f) aims to approve **binding corporate rules** within the meaning of Article 43.

(…)

Consistency Mechanism (2)

Article 62: ***Implementing acts***

1. The **Commission may adopt implementing** acts for:

(a) deciding on the **correct application of this Regulation** in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;

(b) deciding (…) whether it declares draft standard data protection clauses (…) as having general validity;

(c) specifying the format and procedures for the application of the **consistency mechanism** referred to in this section;