Presentation to IAPP
November 18, 2013

EU Data Protection

LORENZ | International Lawyers

Table of Contents

INTRODUCTION
to the draft Regulation

Legislative Agenda

The race to Spring 2014

January 2012	Draft Regulation Proposal by Commission
January 2012 – October 2013	European Parliament and European Council separately debated the draft text
21 October 2013	LIBE Committee 'orientation vote' on compromise text
Expected timeline:	
October – December2013	European Council formulates its position on text for negotiation with Parliament and Commission
Dec 2013/Jan 2014	'Trialogue' negotiations between Commission, Council and Parliament
April 2014	Parliament intends to have 'first reading' vote in plenary session, based on agreement from trialogue if possible
May 2014	European Parliament elections.

Legal Instrument: Regulation or Directive?

- Regulation has direct effect.
- Legal certainty (?).
- Remaining political divide Regulation or Directive.

SCOPE
of the draft Regulation

Territorial and Personal Scope

Old Directive	New Draft Regulation
Processing carried out in the context of the activities of an establishment of the controller on the territory of the Member State	Processing of personal data in the context of the activities of an establishment of the controller **or a processor** in the Union
The controller is not established on Community territory and, for purposes of processing personal data **makes use of equipment,** automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community	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 behavior**

Territorial Scope

Broader application than Directive.

→More non EU-based companies offering services on internet within reach of Regulation.

→LIBE Committee: also non-EU based processors are in scope.

→Not clear: “monitoring”; “individuals residing in EU”; “offering goods or services”.

Personal Scope

Changes to the existing legal framework.

→ Obligations directly imposed on processors.

→ Processors subject to sanctions provided in the Regulation.

Personal Scope

Specific obligations for processors.

Directly liable for:

- Maintaining documentation concerning processing activities.
- Cooperating with supervisory authority.
- Implementing appropriate technical and organizational information security measures.
- Appointing a data protection officer.
- Informing data controller immediately of a data breach.

Personal Scope

Specific new obligations for processors.

- Conducting data protection impact assessment.
- Prior DPA authorization or consultation (where required).
- Complying with the requirements regarding international data transfers.
- LIBE Committee additions: privacy by design, data protection compliance reviews (bi-annually).

Personal Scope

Practical implications.

- Significant increase of enforcement risks and administrative burden.

- Contract negotiations between controllers and processors will become more difficult and important (high sanctions and controllers/processors will be jointly and severally liable).

Material Scope

- No fundamental changes.
- Updates of definitions in light of Working Party positions and online processing (e.g., means of identifying an individual to include location data and online identifiers).
- LIBE Committee: “gender identity” is sensitive information.

SUBSTANTIVE OBLIGATIONS in the draft Regulation

Accountability

Responsibilities and paper trail.

- Data controllers will be obliged to adopt policies and implement measures not just to ensure compliance, but to be able to demonstrate compliance, including:
  - Documentation of all processing operations (also Ps);
  - Appropriate information security (also Ps);
  - Privacy impact assessments (Cs or Ps);
  - Consultation and authorization of DPAs (Cs or Ps);
  - Designation of a DPO where relevant (also Ps).

Accountability

1. Documentation of processing.

- Documentation must be kept available to DPAs.
- Also for processors.
- Obligation watered down by LIBE Committee: "documentation necessary in order to fulfill the requirements laid down in the Regulation".

Accountability

Exemptions to documentation.

- Commission proposal – exemption for companies of fewer than 250 people and processing activities are ancillary activity.
- LIBE Committee: removes exemption.

Accountability

2. Privacy Impact Assessment.

- For processing considered “risky” (e.g. large-scale monitoring or sensitive data processing).
- Controllers or processors.
- LIBE Committee: Risk assessment + privacy impact assessment (stress on information lifecycle management).

Data Minimization

Clarification of Fundamental Principle.

- Personal data ‘shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data.’

Privacy by Design/Default

New Principles.

- **Design:** Taking into account state of the art and cost of implementation, controller obliged to implement measures to ensure compliance with Regulation and protection of data subject rights.
- **Default:** Mechanisms must ensure that default situation is minimum data collection for that purpose – both data amount/retention.
- LIBE Committee: broadens obligation to processors. Obligations apply regardless cost.

Right to be Forgotten

- Right to request (i) erasure of personal data, and (ii) abstention from further dissemination.
- Only in certain cases: (i) data no longer serves purposes; (ii) consent based processing; (iii) right to object (e.g. direct marketing); (iv) illegal processing.
- Obligations to delete and inform third parties without delay.
- Restrictions: e.g. if alternative legal basis to keep the data.

Right to be Forgotten

Concerns.

- LIBE Committee: “obtain from third parties the erasure of any links to, or copy or replication of that data”.
- Technical difficulties/investment and anticipate requirement with processors.

Right to Data Portability

- Right to obtain a copy of data which allows further use by the data subject; and

- Right to transmit personal data and other information processed in automated processing system into another system (e.g. when switching service provider) without hindrance of data controller.

Right to Data Portability

Restrictions.

- Right to obtain a copy of data: only when data are processed by electronic means and in a structured and commonly used format (?) => Commission may clarify; and
- Right to transmit personal data: only if (i) data subject has provided the personal data and (ii) processing is contract or consent based.

FORMAL OBLIGATIONS in the draft Regulation

New Formal Obligations

1) Notification to national DPA abolished.

→ Replaced by obligations regarding accountability.

New Formal Obligations

2) Formal requirements for consent.

- Explicit by default (for sensitive and non-sensitive data).
- Presented distinguishable (e.g. in terms and conditions).
- Withdrawal at any time.
- Not if imbalance in position between controller and data subject (e.g., employment context).

New Formal Obligations

3) Requirement to have clear and easily accessible policies regarding data processing and for the exercise of data subjects' rights.

New Formal Obligations

LIBE Committee Proposal.

→ Introduction of two-step notice procedure with display of basic information at first stage.

ICON	ESSENTIAL INFORMATION	FULFILLED
	No personal data are collected beyond the minimum necessary for each specific purpose of the processing	
	No personal data are retained beyond the minimum necessary for each specific purpose of the processing	
	No personal data are processed for purposes other than the purposes for which they were collected	
	No personal data are disseminated to commercial third parties	
	No personal data are sold or rented out	
	No personal data are retained in unencrypted form	

LORENZ | International Lawyers

New Formal Obligations

4) Data breach notification obligation.

→Extreme broad definition data breach.

→Obligation for data controller to inform (a) the supervisory authority, and (b) the affected data subjects.

→Obligation for data processor to inform data controller.

→LIBE Committee: removed 24 hours deadline => without undue delay. EDPB to issue guidance.

Formal Obligations

5)Prior authorization and prior consultation obligations.

- Prior authorization: for international data transfers based on ad-hoc contracts or if no appropriate safeguards are provided in a legally binding instrument.
- Prior consultation : if (a) PIA indicates high degree of specific risks; or (b) intended processing operation is included in DPA-list as "high risk".

New Formal Obligations

6) Appointment of a data protection officer.

→Data controllers and processors are required to appoint a DPO if, inter alia:

- the processing is carried out by an enterprise employing 250 persons or more; or
- the core activities of controller/processor require regular and systematic monitoring of data subjects.
- LIBE Committee: amended thresholds (e.g. processing of data 5000 individuals over 12 consecutive months, large scale sensitive data processing on children/ employees) + 4 years position (for internal DPO)/2 years if external.

INTERNATIONAL DATA TRANSFERS
in the draft Regulation

International Transfers

- Provisions apply to data controllers and processors.
- Strong focus on onward transfers.
- Evolution: no transfer unless adequate protection => transfer if the conditions in Regulation are fulfilled.

International Transfers

4 types.

- transfers by adequacy decision.
- transfers by way of appropriate safeguards.
- transfers by way of binding corporate rules.
- Derogations.

International Transfers

1. Transfer by adequacy decision.

- By Commission decision.
- Somewhat expanded scope => not only a country, but also a territory within a third country, a processing sector (within that country), or international organization can be adequate.
- LIBE: Sunset clause of 5 years in case of adequacy decision for a specific business sector.

International Transfers

2. Transfers by way of appropriate safeguards.

- BCRs.
- Model contractual clauses (no longer permits).
- Standard model clauses approved by a DPA (in accordance with consistency mechanism).
- Ad hoc contractual clauses.
- Other appropriate safeguards "not provided for in a legally binding instrument".
- LIBE Committee: Adequacy by European Data Protection Seal. 5 Years sunset for current commission decisions. BCR-P deleted.

International Transfers

- Generally the same list as article 26 Directive 1995/46.
- New: “transfer can, under limited circumstances, be justified on a legitimate interest of the data controller or processor, but only after having assessed and documented the circumstances of that transfer.”

International Transfers

Foreign law access requests.

- Situation of disclosure to third countries under foreign law was omitted from Commission's draft.
- Parliament reintroduced this issue in a new Article 43a:
  - No judgment requiring disclosure will be recognized or enforceable unless under a mutual legal assistance treaty.
  - Where disclosure requested by foreign judgment, need prior authorization of DPA.
  - The DPA will assess compliance of disclosure with Regulation and use consistency mechanism if affects data subjects from other member states.
  - Companies must also inform data subjects of the request and obtain authorization.

International Transfers

Is Safe Harbor doomed?

- Following Snowden, overarching concern with protection of EU data in the US.
- Grievances are general, unlikely to crystallize into real action to undermine the Safe Harbor regime.
- Regime may be strengthened in light of the Regulation.

ENFORCEMENT
in the draft Regulation

Enforcement

Enforcement bodies.

- National DPAs.
- European Data Protection Board ("EDPB").
- Commission.
- EDPS.

National DPAs

General.

- DPAs remain but some change in role and responsibilities.
- Rules of establishment and internal procedures remain national.
- Independence requirements for DPAs and members.
- Member states must provide financial resources.

National DPAs

Competences.

- Local territorial enforcement (and vis-à-vis local public authorities).
- Lead DPA for company's "main establishment" in case of multinationals with centralized EU presence.
- LIBE Committee: Lead DPA can ask EDPB to issue opinion who is lead.

National DPAs

Duties.

- General monitoring, complaint investigations as before.
- Specific mutual assistance obligations with other DPAs.
- Specific obligations to ensure consistent application and enforcement (inter alia via "consistency mechanism").
- Specific stress on joint operations of DPAs.
- Issue opinions on draft codes of conduct and approve BCRs.

National DPAs

Powers.

- Notify controllers/processors in case of breach and issue orders to (i) remedy breach, (ii) improve compliance or (iii) conduct consumer breach notifications (LIBE) + temporary or definitive bans on processing.
- Broad investigative powers (including access to any premises and any data processing equipment and means). LIBE: without prior notice (!).

National DPAs

Powers, continued.

- Suspend data flows.
- Issue opinions on any issue related to protection of personal data.
- Issue administrative sanctions, bring violations to attention of judicial authorities and engage in legal proceedings.

European Data Protection Board

European DPA ("EDPB").

- Converts ("replaces") the Art. 29 Working Party into pan-EU DPA.
- Composed of heads national DPAs and EDPS. Commission is not formal member but can participate.

European Data Protection Board

Tasks.

- Consistent application Regulation and promotion cooperation between DPAs (e.g. Role in consistency mechanism, opinions).
- Advice to Commission (e.g., delegated acts, Commission decisions).
- No appeal to EDPB against decisions of (Lead)DPA => local law remedies.

Mutual Assistance

Mutual Assistance (DPA Cooperation).

- DPAs must provide mutual information/ assistance to each other to apply / implement Regulation.
- Commission can determine procedures for cooperation.
- DPA cannot refuse unless:
  - Requested DPA is not competent for the request;
  - Compliance would be incompatible with provisions of Regulation.

Mutual Assistance

Joint Operations.

- In certain cases, DPAs can carry out joint operations.
  - Joint operations = investigations, enforcement measures or other operations where staff of other DPAs are involved.
  - DPAs of other member states have a right to participate in joint operations when processing impacts data subjects on their territory.
- Joint operations will have "host DPA" which assumes responsibility and coordinates the joint operation.

Consistency Mechanism

DPA Draft Measures.

- Prior checking of DPA measures by EDPB.
- If the draft measures intend to provide legal effects and which:
  - concern data processing relating to goods/services in several member states or monitors behavior;
  - affects free movement of personal data within the EU;
  - aims at determining international transfer mechanisms (e.g. DPA standard data protection clauses, ad hoc data transfer agreements, approvals for BCRs).

Consistency Mechanism

Consistency Mechanism – Additional Grounds.

- Upon request of a DPA or EDPB.
- Upon request Commission.

Consistency Mechanism

EDPB Opinion.

- The EDPB will issue an opinion on the matter within one week of the provision of information.
- This opinion will be adopted within one month.
- The DPA issuing the draft measure and the lead DPA have two weeks to maintain or amend its draft measure.
- LIBE Committee: Amends process and distinguishes between “measures of general application” and “individual cases”.

SANCTIONS, REMEDIES, LIABILITY
in the draft Regulation

Administrative Sanctions

Regime proposed by Commission.

- New sanctions have "teeth" to ensure compliance.
- DPA "shall" impose fines for negligent or intentional violations:
  - Up to EUR 250,000 or 0.5% of annual global turnover for companies for lesser offenses (e.g. not promptly responding to with data subjects requests);
  - Up to EUR 500,000 or 1% of annual global turnover for companies for medium offenses (e.g. not maintaining required documentation or not providing information to data subjects); and
  - Up to EUR 1,000,000 or 2% of annual global turnover for companies, for most serious offenses

Administrative Sanctions

Regime proposed by Commission.

- Each DPA empowered to issue fines.
- Some DPA has discretion to ensure sanctions are effective, proportionate and dissuasive.
- The amount of fine is determined based on the following criteria:
  - nature, gravity and duration of breach;
  - character of breach (negligent versus intentional);
  - degree of responsibility of natural/legal person and previous breaches;
  - technical and organizational measures implemented; and
  - degree of cooperation with DPA to remedy breach.

Administrative Sanctions

Regime proposed by LIBE Committee.

- Even more aggressive sanctions:
  - DPA shall impose at least one of the following:
    - Written warning
    - regular data protection audits
    - fine of up to **EUR 100,000,000 or up to 5% of the annual global turnover**
  - Companies with EDP Seals will only be fined in cases of intentional or negligent non-compliance.
  - Fines may take into account certain factors, e.g. Nature, gravity, intentional or negligent character, repetitive nature, etc.

Remedies and Liabilities

Right to lodge complaint before DPA.

- Every data subject or organization representing individuals' interests.
- In any Member State.
- Complaint can also concern data pertaining to other individuals than complainant.

Remedies and Liabilities

Right to judicial remedy against DPA.

- Each individual / company has right to judicial remedy against a DPA.
- Normally, the local courts will have jurisdiction. However, in case of multi-jurisdictional issues, data subject may ask local DPA to bring proceedings on its behalf against the competent DPA in other Member State.

Remedies and Liabilities

Compensation, Liabilities & Remedies.

- Individuals and organization/association representing individuals can initiate proceedings.
- Competent courts are the courts where controller or processor has establishment; alternatively, courts of habitual residence of the data subject.
- harmed by unlawful processing can claim compensation from controller/processor for damages.
- Joint and several liability where there is more than one controller or processor.

WHAT NEXT?

Delegated & Implementing Acts

- Critique for leaving too much uncertainty: contains 26 opportunities for Commission to later adopt Delegated Acts and 22 provisions contemplating Implementing Acts.
- Both the Parliament and the Council have proposed the removal of most of these powers, and instead increase the role of the European Data Protection Board.

Being Prepared

- Once the Regulation is passed there will likely be a two year period before it comes into force.
- As soon as there is a clear text, businesses should begin preparation – 2 years will not be much time considering the significant changes contemplated!

Take-away for US companies

- Lower threshold for applicability of EU laws.
- Privacy higher priority for compliance.
- Greater administrative burden – documentation obligations, appointment of DPO.
- New obligations for processors with EU establishments.
- Greater flexibility for international transfers.
- More harmonization...?

We appreciate the opportunity to be of service to you.

Lorenz
Regentlaan 37-40 Boulevard du Régent
1000 Brussels, Belgium
Telephone +32 2 239 2000 - Fax +32 2 239 2002
www.lorenz-law.com

LORENZ | International Lawyers