Aspects of a new Data Protection Law

Mathias Cellarius, SAP AG

Milestones of the Reform of EU Data Protection Law

- **Current Data Protection Directive 95/46/EC dates back to 1995.**
- **Commission officially started process for a reform of the data protection law in 2010.**

  Goals:

  - Update and modernise the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights in the future.
  - Protect individuals' data in all policy areas, including law enforcement, while reducing red tape for business and guaranteeing the free circulation of data within the EU.
  - Data protection rules for the digital age.
- **Jan 2012: Commission proposal for a Data Protection Regulation.**
- **March 2014: EU Parliament voted to support Data Protection Regulation; but has proposed changes.**

Advertised Changes

- **One continent, one law.**
- **One stop shop for data controllers and for data subjects**
- **Less bureaucracy in exchange for increased responsibility and accountability of data controllers.**
- **More significant enforcement powers of supervisory authorities.**
- **Joint responsibility of controllers and processors.**
- **Right to data portability.**
- **Right to be forgotten.**
- **Privacy by design / Privacy by default.**
- **Stronger focus on consent requirement.**

Business Impacts: One Continent – One Law

- **Directive → Regulation:**

  “27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year.”

  (press release of the EU Commission of Jan. 25, 2012)

- **A regulation, by definition of Article 288 of the Treaty on the Functioning of the European Union, is directly applicable law in all Member States**
- **However, no guarantee for a uniform data protection law. The proposed Data Protection Regulation provides for national “detailing”, e.g. Art. 80.**

Business Impact: One Stop Shop

- **Data controllers and data processors will only have to deal with a single national data protection authority in the EU country where they have their main establishment.**

  (but: the point of reference is the respective processing operation).

- **Likewise, people can refer to the data protection authority in their country, even when their data is processed by a company based outside the EU.**

- **Stronger cooperation between the national supervisory authorities, incl. mutual assistance, joint operations and a consistency mechanism shall ensure a consistent application of the law throughout the EU.**

Business Impact: Less bureaucracy vs. Increased Accountability

- A **level playing** field for businesses through one single law applicable to any business across the EU. The Commission expects businesses to **save up to €2.3 billion/year.**
- "Simpler, clearer and stronger" rules are expected help build individuals' **trust** in emerging businesses, particularly online.
- Companies are required to **proactively take measures to ensure compliance** with data protection law:
  - Documentation of processing operations (n/a if < 250 employees, unless processing of personal data is a main business activity (i.e. not only ancillary to the company's main activities)).
  - Cooperation with supervisory authority; security breach notifications
  - Implementation of adequate technical and organisational security measures
  - Communication of security breaches to data subjects, unless company can demonstrate to supervisory authority appropriate technological protection measures were in place
  - Data protection impact assessment mandatory prior to high risk processing operations (profiling, sensitive data); approval by supervisory authority may be required
  - Commissioned data processing: monitoring and documentation requirements.
  - Need to have a data protection officer (n/a < 250 employees + ancillary processing)

Business Impact: enforcement powers of supervisory authorities

Supervisory authorities have the powers:

- **To request information**
- **To order a controller or processor to remedy a breach and to improve the protection**
- **To enforce legitimate requests of a data subject**
- **To order the rectification, erasure or destruction of data**
- **To stop and ban processing operations and data flows to a recipient in a third country or to an international organisation**
- **To enforce compliance, by administrative enforcement and also in court**
- **To issue opinions and to inform governments, parliaments and other political institutions and the public**

Business Impact: Remedies, Liability and Sanctions (1)

1) **Data subjects** have rights**:**

- To information, recificiation, to be forgotten / erasure, data portability, object, not be subject of profiling; **against data controller**
- To lodge a **complaint with any supervisory authority**
  - To a **judicial remedy against decisions of a supervisory authority** concerning them.
  - To a **judicial remedy obliging the supervisory authority to act on a complaint** in the absence of a decision necessary to protect their rights or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint.
  - **To assistance by its supervisory authority against the decision of another supervisory authority:** A data subject that is concerned by a decision of a supervisory authority in another Member State may ask the supervisory authority where the data subject has its habitual residence to bring proceedings on its behalf against the supervisory authority in the other Member State.
- To a **judicial remedy against a controller or processor**
  - **Joint and several liability** among all involved controllers and processors
  - But: A controller or processor **may be exempted from this liability** (by the court), in whole or in part, if it proves that they are not responsible for the event giving rise to the damage.

Business Impact: Remedies, Liability and Sanctions (2)

2) Properly constituted **bodies, organisations or associations which aim to protect data subjects' rights and interests concerning the protection of their personal data** have the rights:

- **To act on behalf one or more data subjects** (Complaints to supervisory authorities; judicial remedies against supervisory authorities; judicial remedies against controllers and processors.
- **Independently of a data subject's complaint:** right to lodge a complaint with a supervisory authority in any Member State, on the consideration that a personal data breach has occurred.
  - To a judicial remedy against decisions of the respective supervisory authority.

3) Each **supervisory authority** has the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of the Regulation or to ensure consistency of the protection of personal data within the EU.

Business Impacts: Remedies, Liability and Sanctions (3)

Commission Proposal:

“The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently (…)”

European Parliament Vote:

To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:

a) a warning in writing in cases of first and non-intentional non-compliance;

b) regular periodic data protection audits;

c) a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater

Business Impact: Right to data portability

The right to data portability has two elements:

- individuals whose personal data are processed electronically and in a “structured and commonly used format” are given the right to **obtain a copy** of that data for further use.
- Individuals have the right to **transmit their personal data from one provider to another**.

The Commission may define the electronic format in which data must be provided as well as standards for a transmission from one provider to another.

Business Impact: Right to be forgotten

- The right to be forgotten is **in addition to the right of erasure and abstention from further dissemination**. It kicks in **where the controller has made the personal data public**.
- The controller must take **“all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data.”**

Business Impact: New rules for consent

- **Art. 7 (4) :** Consent shall not provide a legal basis for the processing, where there is a **significant imbalance** between the position of the data subject and the controller.
- Can companies still rely on a data subject's consent or do they have to fall back on other legal bases to legitimize processing operations? How about standard internet service offerings? Employers?
- How about consent templates?

Business Impact: Other not (fully) yet resolved topics

- **Complex (sub-)processing structures: how can controllers meet their legal responsibilities to monitor and ensure the processor‘s and its subprocessors‘ compliance?**
- **Certification as a solution?**
- **Cross border transfers for processing: No clarification on the use of non-European subprocessors by a European processor.**

Let‘s dicuss!

- The draft Regulation is strongly oriented at the current Directive. **It‘s an evolution, not a revolution** – while the technical evolution has become a revolution.
- **Pressing questions**, such as international cooperation and issues like the NSA scandals **have not been answered.** International businesses are risking to be caught between a rock and a hard place more than before.
- **Better this Regulation than no Regulation?** Do one continent – one law and one-stop shops alone provide enough value and benefit for all market participants to support the rapid enactment of the Regulation?
- **Work needs to go on**. If “data” is the most important economical resource of the 21 century, and if development continues in an exponential way, can can there be a once-for-all-and-for-all-times solution?

Thank you

Contact information:

Mathias Cellarius
SAP AG
Global Legal
Dietmar-Hopp-Allee 16, 69190 Walldorf/Germany
mathias.cellarius@sap.com

© 2014 SAP AG or an SAP affiliate company. All rights reserved.

© 2014 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.