Reforming EU Data Protections… No Ordinary Sequel

Eric A. Hibbard, CISSP, CISA
Thomas Rivera
Hitachi Data Systems

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Abstract

Reforming EU Data Protections…No Ordinary Sequel

After reviewing the diverging data protection legislation in the EU member states, the European Commission (EC) decided that this situation would impede the free flow of data within the EU zone. The EC response was to undertake an effort to "harmonize" the data protection regulations and it started the process by proposing a new data protection framework. This proposal includes some significant changes like defining a data breach to include data destruction, adding the right to be forgotten, adopting the U.S. practice of breach notifications, and many other new elements. Another major change is a shift from a directive to a rule, which means the protections are the same for all 27 countries and includes significant financial penalties for infractions.

This session explores the new EU data protection legislation and highlights the elements that could have significant impacts on data handling practices.

Privacy Versus Data Protection

Privacy

The appropriate use of personal information under the circumstances. *What is appropriate will depend on context, law, and the individual's expectations; also, the right of an individual to control the collection, use and disclosure of information.*

- Source: International Association of Privacy Professionals (IAPP) Glossary

Data Protection

The management of personal information. *In the United States, "privacy" is the term that is used in policies, laws and regulation. However, in the European Union and other countries, the term "data protection" often identifies privacy-related laws and regulations.*

- Source: International Association of Privacy Professionals (IAPP) Glossary

Personal Data: The Current EU Definition

*Personal data shall mean **any information relating to an identified or identifiable natural person** ("data subject"); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*

- Source: EU Directive 95/46/EC – Article 2(a)

- ***Any information***
  - **Nature** – both objective (fact) and subjective (opinion),
  - **Content** – concept of private and family life must be widely interpreted,
  - **Format** – information in any form. Paper, electronic records, CCTV, telephone calls, etc.
- ***Relating to*** – information must be about an individual. Information that relates to objects, process or event may also constitute personal information. For example an individual owns a car.
- ***An identified or identifiable*** – a natural person is identifiable when, although the person has not been identified, it is possible to identify him/her.
- ***Natural person*** – all natural persons regardless of their country of residence. Typically relates to living people.

EU Directive Versus Regulation

- ***Directive***
  - Specific objectives that must be reached and Member States need to adopt national implementation legislation
  - Member States left with the choice of form and method of implementation
  - Language in Directives tend to be more general to allow Member States to adapt in their legislation

- ***Regulation (Rules)***
  - Directly applicable to all Member States
  - Do not require any additional implementation in national legislation
  - Apply in all Member States in the same wording and scope
  - Law across ***all*** Member States as written

Proposed Reform of the EU Data Protection Directive

The Need for Reform

- In 2009, the European Commission (EC) began a process of reviewing the general EU legal framework on the protection of personal data
- The main policy objectives:
  - ***Modernize the EU Legal System*** for the protection of personal data, in particular to meet the challenges resulting from globalization and the use of new technologies
  - ***Strengthen Individuals' Rights***, and at the same time reduce administrative formalities to ensure a free flow of personal data within the EU and beyond
  - ***Improve the Clarity and Coherence*** of the EU rules for personal data protection and achieve a consistent and effective implementation and application of the fundamental right to the protection of personal data in all areas of the Union's activities

Proposed Changes

- January 25, 2012 – the EC proposed "***a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy***"
  - ***Regulation*** (replacing Directive 95/46/EC) "*General Data Protection Regulation*" – to set out a general EU framework for data protection. This regulation would make limited technical adjustments to the e-Privacy Directive (2002/58/EC). Total of 91 Articles in the Proposed Regulation.
  - ***Directive*** (replacing Framework Decision 2008/977/JHA) to set out rules on the protection of personal data processed for the purposes of prevention, detention, investigation, or prosecution of criminal offences and related judicial activities.

Single Set of Rules

- Will replace the existing 28 country specific laws with a single set of EU rules on data protection.
- Companies will only have to deal with a single national Data Protection Authority (DPA) – in the EU country where they have their main establishment
- Individuals will have the right to refer cases to their home national DPA, even when their personal data is processed outside their home country
- EU rules will apply to companies not established in the EU, if they offer goods or services in the EU or monitor the online behavior of citizens.
- Abandons the presumption that personal data may not be transferred absent an "*adequate level of protection*" in the recipient country, and sets for general principles that must be fulfilled when data are transferred outside the EU
- ***Implement privacy by design/privacy by default.***

Potential Impacts on non-EU Companies
(that would be subject to the Regulation)

"Personal Data" Redefined

- Expansion of "***Personal Data***" Definition
  - ***Any information relating to a data subject***
  - It is independent of whether it relates to ones private, professional or public life
  - It can be anything from a name, a photo, an email address, your bank details, your posts on social networking websites, your medical information, or your computer's IP address
- "***Data subject***" definition broadened
  - Identified by means reasonably likely to be used by the data controller or by any other natural or legal person,
  - By reference to not just an identification number but also to location data and online identifiers, or
  - To additional factors like genetic and mental identity, among other factors.

Express Consent

- Covered businesses are required to obtain (and not assume) the ***express consent*** of the data subject
  - to the processing of his/her personal data for one or more **specific purposes**
  - unless processing is required for certain limited purposes such as compliance with a legal obligation of the business or to protect the vital interests of the data subject
  - ***The data controller bears the burden of proof for the data subject's consent to the processing of their personal data***
- The data subject may withdraw the consent at anytime; ***the right to be forgotten (the right to erasure)***.
- Consent is essentially not valid where there is an "*imbalance*" between the position of the data subject and the business.

NOTE: Amendments have been proposed, so some of this may change.

Breach Notification Requirement

- ***Personal data breach*** *– a breach of security leading to the accidental or unlawful* ***destruction***, ***loss***, ***alteration***, *unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*

- Businesses must notify the ***supervisory authority*** (i.e., the public authority established by each Member State) of a personal data breach "***without undue delay and, where feasible, not later than 24 hours"*** after becoming aware of the breach.
- Companies must also notify the ***affected data subject*** of a personal security breach "***without undue delay***" if the personal security breach "*is likely to adversely affect the protection of the personal data or privacy of the data subject*."

NOTE: Amendments have been proposed, so some of this may change.

Policies and Measures

- Businesses must adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the Regulation
- Businesses must have transparent and easily accessible policies regarding the processing of personal data that are clearly presented to data subjects that:
  - provide the identity and contact information of the business,
  - identify the purpose of processing the personal data,
  - set forth the data subject's right to access, correct or have the personal data deleted,
  - set forth the right of the data subject to complain to supervisory authority,
  - specify the period during which the personal data will be stored by the business,
  - and specify whether the personal data will be disclosed to third parties and/or transferred to third countries

Data Security Obligations

- Businesses are required to ***implement appropriate technical and organizational measures*** "*to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation*."
- ***Privacy by design*** (and ***privacy by default***) principle – data protection safeguards are factored into the planning stage of procedures and systems
- ***Right to data access, correction, and erasure***
- ***Right to transfer data*** from one electronic systems to another and to obtain a copy of data where it is processed electronically and in a commonly used format
- Companies will be ***obligated to strengthen their security*** measures to prevent and avoid breaches
- ***Special protections for children*** and their personal data (e.g., verifiable parental consent, right to be forgotten)

Binding Corporate Rules (BCRs)

- BCRs are the tool used by companies with global operations to transfer personal data of EU residents within their corporate group to entities located in countries which do not have an adequate level of data protection.
  - Typically form a stringent, intra-corporate global privacy policy that satisfies EU standards
  - Should be seen as a framework having different elements (Internal legal agreement, Policies, training, audit, etc.) providing compliance
- BCRs will no longer need to be approved by each Data Protection Authority in each applicable EU Member State.
  - Only need to be approved by one authority
  - The BCRs will be recognized by the rest of the authorities in each applicable Member State.
- The approved BCRs would also cover third parties that process personal data of EU residents on behalf of the business, such as cloud service providers, for example.

Data Protection Impact Assessment

- Required for businesses with processing operations that "***present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes***"
- Must describe the processing foreseen, risks to data subject rights and freedoms, means of addressing these and those designed to protect personal data, and demonstrate compliance with the Rules.
- The views of data subjects on the processing must also be sought.
- Accomplished by or on behalf of the data controller (i.e., at its expense).
- Examples of these activities include (not limited to):
  - monitoring publicly accessible areas
  - use of the personal data of children
  - use of genetic data or biometric data
  - processing information on an individual's sex life
  - the use of information regarding health or race
  - an evaluation having the effect of profiling or predicting behaviors

Data Protection Officer (DPO)

- Requirement for organizations to ***appoint a DPO with expertise in privacy regulations*** if it processes data related to about 5,000 or more "data-subject" individuals in some way
  - DPOs must have expert knowledge of data protection law and practices and conduct data-privacy assessments and ensure appropriate policies are in place
  - DPOs are to be appointed for four years at the business and must be independent and report to upper management on topics such as compliance with data-privacy regulation
  - DPOs must be known to the appropriate government regulatory agencies in Europe and the public; decision to not appoint a DPO must be communicated to the public sources
- Responsible for monitoring data processing activities
- **Significant shortages are anticipated for these privacy experts**

NOTE: Amendments have been proposed, so some of this may change.

Transfers of Data to Third Countries

- Restrictions on the transfer of personal data to third countries that do not offer an adequate level of protection remain in place
- International data transfers are possible if one of the following mechanisms are in place:
  - Binding Corporate Rules (BCRs)
  - "*Standard data protection clauses*" approved by the EC (the counterpart of the present "*standard contractual clauses*").
  - Standard data protection clauses adopted by a DPA in accordance with the consistency mechanism
  - "*Ad hoc*" contractual clauses authorized by a DPA
  - Other appropriate safeguards "*not provided for in a legally finding instrument*."

Significant Penalties

- Introduces the ability of each supervisory authority to impose fines
- Penalties for violations of the Regulation range from a written warning to fines for intentional or negligent conduct of anywhere from **€1,000,000** or **5%** of the annual worldwide turnover of a company.
- **Severe Offenses include** (among others):
  - Not adopting internal policies or does not implement appropriate measures for ensuring and demonstrating compliance
  - Not alerting on, or failing to do a data breach notification in a timely manner
  - Not carrying out a data protection impact assessment
  - Not designating a Data Protection Officer (DPO)
  - Carrying out a data transfer to a third country not allowed by an adequacy decision
- The administrative sanction "*shall be in each individual case **effective, proportionate and dissuasive***."

NOTE: Amendments have been proposed, so some of this may change.

Wrap Up

The Road to Approval

- In May 2012, the European Parliament held the first stakeholder meeting
- In early 2013, key committees voted their opinions on the draft (including amendments)
- Throughout 2013 the LIBE committee received and considered over 4000 proposed amendment (making it the most heavily lobbied piece of EU legislation ever)
- In October 2013, the LIBE committee voted and approved a revised version of the Regulation
- In March 2014 the LIBE text was voted and approved by the whole Parliament
- The Council of Minister (representing the Governments of each Member State) is expected to come to its own agreement on the text as it is, or more likely its own revision by Autumn of 2014 at the earliest
- Triparite negotiation between the Commission, Council of Ministers, and the Parliament will occur after each body has agreed to its own position
- It is generally expected that the final agreement will be reached at some time in 2015

Summary

- ***The protection of personal data is a fundamental right for all Europeans*** (Article 8 of the EU's Charter of Fundamental Rights and by the Lisbon Treaty)
- When the rules are ultimately approved (2015), there will be a transition period (24 months) before enforcement starts (2017)
- Elements of the Regulation may be adopted early (e.g., the court case decided the right to be forgotten issue)
- There are indications that the existing **U.S.-EU Safe Harbor** may still have some value

Conclusions

- Until the Snowden adventure there were signs of softening of the Rules, the LIBE committee's revised draft has given indications that this is less likely going forward

- According to the ABA Business Law Section, don't wait until the Rules are approved:
  - *Put the General Data Protection Rules on Your Radar*
  - *Audit Risks for Potential Data Protection Violations*
  - *Incorporate Data Protection into Compliance Programs*
  - *Make Sure Proper Consent is Obtained*
  - *Prepare for Data Breaches*

Attribution & Feedback

The SNIA Education Committee thanks the following individuals for their contributions to this Tutorial.

Authorship History

Eric A. Hibbard – April 2013

Updates (Aug-2014):
- **Eric A. Hibbard**
- **Thomas Rivera**
- **Gene Nagle**

Additional Contributors

SNIA Security TWG

SNIA Data Protection & Capacity Optimization (DPCO) Committee

Please send any questions or comments regarding this SNIA Tutorial to ***tracktutorials@snia.org***