Privacy vs Data Protection: The Impact of EU Data Protection Legislation

Thomas Rivera, CISSP

Security & Privacy Consultant, Cyber adAPT, Inc.

Co-Chair, Data Protection & Capacity Optimization (DPCO) Committee – SNIA

Secretary, Cybersecurity & Privacy Standards Committee - IEEE

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

Privacy vs Data Protection:
The impact of EU Data Protection Legislation

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 28 countries and includes significant **financial penalties** for infractions.

This tutorial 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 used in policies, laws and regulation
  - In the European Union (EU) and other countries, the term "data protection" often identifies privacy-related laws and regulations

Source: International Association of Privacy Professionals (IAPP) Glossary

Data Protection: Various Definitions

- **Data Protection** (Storage)

  Assurance that data is not corrupted, is accessible for authorized purposes only, and is in compliance with applicable requirements

  Source: Storage Networking Industry Association Dictionary

- **Data Protection** (Security)

  The implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data

  Source: ISO/IEC 2382:2015

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 & method of implementation
- Language in Directives tend to be more general to allow Member States to adapt into their legislation

Regulation

- Directly applicable to ***all*** Member States
- Does 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

New EU Data Protection Regime

- ***EU Regulation*** 2016/679 (replacing Directive 95/46/EC) "*General Data Protection Regulation*" (GDPR)
  - To set out a general EU framework for data protection
  - Would make limited technical adjustments to the e-Privacy Directive (2002/58/EC)
  - Total of 91 Articles in the Proposed Regulation

- ***EU Directive*** 2016/680 (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

“Personal Data” Redefined

- Expansion of “**Personal Data**” Definition
  - ***Any information relating to a data subject***
  - Independent of whether it relates to ones private/professional/public life
  - 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 things like:
    - location data and online identifiers
    - Genetic identity
    - Mental identity
    - Others…

EU - General Data Protection Regulation (GDPR) Summary (1 of 5)

Express Consent

- Covered businesses are required to obtain (and not assume) the ***express consent*** of the data subject
- 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

Breach Notification Requirement

- Businesses must notify the ***competent supervisory authority within 72 hours*** of a personal data breach after becoming aware of breach
- If a breach is likely to result in a high risk for individuals' rights and freedoms, companies ***must also notify the affected data subject*** of the data breach without undue delay

EU - General Data Protection Regulation (GDPR) Summary (2 of 5)

Policies and Measures

- Businesses are required to ***implement appropriate technical and organizational measures***
- ***Privacy by design*** (and ***privacy by default***) principle
- ***Right to data access, correction, and erasure***
- ***Right to transfer data***
- ***Special protections for children*** and their personal data

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
- ***BCRs will no longer need to be approved by each Data Protection Authority in each applicable EU Member State***

EU - General Data Protection Regulation (GDPR) Summary (3 of 5)

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, risks to data subject rights & freedoms, means of addressing these & those designed to protect personal data, and demonstrate compliance
- The views of the 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 (but not limited to):
  - Monitoring publicly accessible areas
  - Use of personal data of children (under 13-16 years of age)
  - 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

EU - General Data Protection Regulation (GDPR) Summary (4 of 5)

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
- Responsible for monitoring data processing activities
- **Significant shortages are anticipated of these privacy experts**

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 items are in place:
  - Binding Corporate Rules (BCRs)
  - "*Standard data protection clauses*" approved by the EC
  - 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 binding instrument"

EU - General Data Protection Regulation (GDPR) Summary (5 of 5)

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 maximum, up to a maximum of ***€20,000,000*** or ***4% of a company's worldwide global turnover*** (preceding financial year), which ever is higher
- ***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***"

Wrap Up

The Road to Approval

- In May 2012, the European Parliament held the first stakeholder meeting
- In early 2013, key committees voted 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) was expected to came to its own respective agreement on the text in late 2015
- Triparite negotiation between the Commission, Council of Ministers, and the Parliament took place after each body has agreed to its own position in early 2016
- The final agreement was reached in early April, 2016, and went into effect (after the 24-month transition period) on May 25, 2018

Note: The committee of the European Parliament responsible for reviewing the draft proposals is the Committee on Civil Liberties, Justice and Home Affairs ("LIBE")

Summary

- ***The protection of personal data is a fundamental right for all EU folks***
  - (Article 8 of the EU's Charter of Fundamental Rights and by the Lisbon Treaty)
- Now that the “GDPR” and Directive 2016/680 are approved (April, 2016), and published in May, 2016
  - Enforcement starts on May 25, 2018, (24 months after transition period)
- Elements of the Regulation may be adopted early (e.g., the court case decided the right to be forgotten issue)
- The **U.S.-EU Safe Harbor** has been struck down as of October, 2015, and the new agreement (“**EU-US Privacy Shield**”) was passed in March, 2016
  - Challenges are still being negotiated on both sides of the Atlantic

How Non-EU Businesses are Affected

Example: Google was sued in the EU (Ruling came in March, 2015)

- The case was brought by three British users (2011 - 2012)
- The claim was alleged clandestine tracking and collation of information on their internet usage on the Apple Safari browser without their knowledge
- The users claim the information obtained by Google “was aggregated and sold to advertisers who used its DoubleClick advertising service.”
- Google was able to obtain information in areas including:
  - Websites visited
  - User’s interests, hobbies, shopping habits, social class, political & religious beliefs, health, financial standing, etc.

http://www.bailii.org/ew/cases/EWCA/Civ/2015/311.html

https://www.scmagazineuk.com/google-vidal-hall-opens-the-floodgates-to-data-breach-compensation/article/537060/

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
Updates (Jan-2015): Eric A. Hibbard
Thomas Rivera
Updates (Aug-2015): Eric A. Hibbard
Thomas Rivera
Updates (Oct-2015): Eric A. Hibbard
Thomas Rivera
Updates (Nov-2015): Eric A. Hibbard
Thomas Rivera
Updates (Feb-2016): Eric A. Hibbard
Thomas Rivera
Updates (Aug-2016): Eric A. Hibbard
Thomas Rivera
Updates (Aug-2017): Eric A. Hibbard
Thomas Rivera

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