GDPR: A QUICK OVERVIEW

2018 – Get ready now.

29 June 2017
Presenters

Charles Barley
Director, Risk Advisory Services
Charles Barley, Jr. is responsible for the delivery of governance, risk and compliance (GRC) services. He has over 15 years of consulting experience and has served several multinational financial services and public sector organizations.

Alain Marcuse
Director, Risk Advisory Services
Alain Marcuse provides security and privacy consulting to clients in a broad spectrum of domains, including security assessments, risk management, penetration testing, compliance frameworks and strategic advisory services.

Steven Snaith
Partner, Technology Risk Assurance
Steven Snaith has 15 years of experience in technology risk audit and has been responsible for a wide range of clients within the private and public sectors.
Agenda

• What is the GDPR?
• Who does GDPR apply to?
• Learn from the European experience
• Develop a road map for compliance
What is GDPR?

• European Union General Data Protection Regulation – “EU GDPR”

• New data protection law adopted by the EU in April 2016, intended to bolster data privacy protections for EU residents.

• Companies, government agencies, and non-profits interacting with EU residents have until May 2018 to comply.
Who does GDPR protect?

- The European Union. Consisting of 28 member states: Spain, UK, Ireland, France, Germany, Italy, and Sweden, among others
- Some island nations such as the Canary Islands, Azores, and others
- Organizations storing, transmitting or processing data for individuals residing in any of these countries
Who does GDPR apply to?

• To determine if GDPR affects your organization, you need to ask questions such as:
  
  - Do you offer goods and services to EU residents?
  - Do you rely on third parties that store or transmit data to/from the EU?
  - Do you collect, transmit, or process data pertaining to EU residents?

• It does not matter whether the services are free
• It does not matter whether your company operates in the EU
7 core principles

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

A few implications follow . . .
Accountability

• Organizations must demonstrate “privacy protection by design and by default.”

• Must appoint Data Protection Officer (DPO) if the:
  – Organization processes data of more than 5,000 individuals a year OR
  – Is active in regular and systematic monitoring of individuals OR
  – Processes data which is sensitive

• Sanctions (more on that later)
Consent

• Burden of consent now states that:
  – Organizations must now prove genuine, explicit consent for data gathered
  – Consent must be purpose-limited
  – Must allow withdrawal of consent at any time
  – In some instances, consent must be down to business process level
  – In some instances (or countries), must gather consent for individuals as young as age 13 (through their parents)
Right to be forgotten

• Mandatory right to erasure – organizations must give individuals the right to request erasure of their data if:
  – Individual withdraws consent
  – Data is no longer needed to achieve the purpose it was collected for
  – Data in question was obtained through unlawful processing
Data portability

• Individuals have the right to transport all of their personal data to another organization (even a competitor):
  – Organizations must provide individuals with their data in a machine-readable format
  – Where feasible, the organization must facilitate electronic transfer of personal data
Breach notification

- Organizations are now under legal obligation to notify local authorities within 72 hours if EU resident data is lost
  - Only exception is if the data was encrypted
  - Organizations have to inform individuals if “adverse impact” is determined from the breach

- Service providers (data processors) now have obligations to data controllers
Penalties for non-compliance

If organizations do not comply, they face a maximum fine of:

- 4% of their global revenue
- €20 million

...whichever is higher
The European perspective: Evolving legislative landscape

1995 Data Protection Directive

- Different rules apply in different countries
- Organizations had to work with authorities in different countries
- Only EU companies had to comply
- Consent for collection and processing of data is assumed
- Applies only if person can be directly identified from data
- Directive = need member states to legislate; not automatic enforcement

General Data Protection Regulation

- Mostly, a single-set of rules applies across the EU
- Organisations work with one central authority in chosen country – fixed upon their main base
- Some non-EU companies will have to comply if offering services to EU residents
- Consent for collection and processing of data must be explicitly given
- Applies if person can be indirectly identified
- Regulation = immediately enforceable across all member states as national law
<table>
<thead>
<tr>
<th>European perspective – key issues we are seeing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carry out an information audit (data held how long for, why, where, how is it shared, and is it still needed) and data flow mapping exercise</td>
</tr>
<tr>
<td>Update all policies and procedures to reflect changes</td>
</tr>
<tr>
<td>Update or create information asset register</td>
</tr>
<tr>
<td>Form a data governance group</td>
</tr>
<tr>
<td>Implement / review breach notification procedures and incident management plans</td>
</tr>
<tr>
<td>Review impact of data retention e.g. on archiving</td>
</tr>
<tr>
<td>Review IT development and purchase procedures – ‘privacy by design’</td>
</tr>
<tr>
<td>Consider the position of the existing DPO within the management structure</td>
</tr>
<tr>
<td>Consider and record lawful bases for processing</td>
</tr>
<tr>
<td>Service provider / third-party contracts – are changes required to current agreements with data processors</td>
</tr>
<tr>
<td>Check accountability in this area is clear and precise</td>
</tr>
<tr>
<td>Check how consent is obtained? Are changes to this process required? Retain records of consent</td>
</tr>
</tbody>
</table>
Roadmap: How do I manage the GDPR puzzle?
How should I think about data privacy?

- Privacy is a business issue
- Privacy is enabled by information security
- Privacy is more than a compliance activity
What tactical items should I consider?

To understand the risk associated with data protection, organizations must first begin by agreeing that data privacy is a multi-faceted business issue regarding the collection, use and disclosure of personally identifiable information.

**People**
- Who are the key process and control owners and what are their organizational roles?
- What information flows from one person to another?
- How are people trained to maintain adequately execute within the processes?

**Process**
- What processes govern the flow of information?
- Do processes govern the disclosure of data to third parties?
- Has the organization established a data privacy impact assessment program?
- Which internal and external systems maintain personal information?
- Has the organization deployed a data loss prevention solution?
- Has the organization developed a data consent mechanism?

**Technology**
- What processes govern the flow of information?
- Do processes govern the disclosure of data to third parties?
- Has the organization established a data privacy impact assessment program?
- Which internal and external systems maintain personal information?
- Has the organization deployed a data loss prevention solution?
- Has the organization developed a data consent mechanism?

**Tactical considerations**

**Governance**
- Privacy officer
- Privacy policies
- Awareness program

**Administration**
- Privacy risk assessments
- Data protection framework
- Data erasure

**Management**
- Data protection requirements
- Incident response plan
- 72hr breach notification
How do I get my house in order?

Privacy is a business issue

**Identify**
- Conduct an enterprise privacy assessment
- Develop a data inventory
- Identify the flow of data (e.g., systems)
- Categorize the location and storage of data

**Diagnose**
- Review the information protection framework (e.g., policies, procedures, etc.)
- Analyze the organization’s data retention strategy
- Review the third party data sharing practices
- Assess the vendor management posture

**Implement**
- Implement a governance structure and privacy officer
- Design / enhance privacy policies and information handling procedures
- Develop a process / mechanism to obtain and manage consent
- Implement a data breach notification and incident response program
- Establish an ongoing data privacy impact assessment program
- Launch a privacy awareness and training program
Wrap-up

• While GDPR represents an important step forward for individual privacy rights, it will require potentially vast changes and significant investments by organizations around the world to comply

• RSM’s IT privacy methodology can be leveraged to assess those gaps and provide guidance on the GDPR roadmap