Cyber Security and The General Data Protection Regulation

Obligations, Challenges and Solutions

Wim Nauwelaerts
Partner
Hunton & Williams

Stewart Room
Partner, Global Head of Cyber Security and Data Protection
PwC Legal

Ann Cavoukian
Executive Director of the Privacy and Big Data Institute
Ryerson University

Gershon Janssen
Chairman
OASIS Board of Directors
Cyber Security and the General Data Protection Regulation – Obligations, Challenges and Solutions

Wim Nauwelaerts
Partner
Global Privacy & Cybersecurity Practice
Hunton & Williams
Brussels
+32 (0)2 643 58 00
wnauwelaerts@hunton.com

9 September 2016
General Data Protection Regulation (EU) 2016/679 (GDPR) – in a Nutshell

- Entered into force on May 25, 2016; Replaces Data Protection Directive 95/45/EC
  - Update was needed to keep up with technological developments
- As a regulation, the GDPR will be directly applicable in each EU Member State from May 25, 2018, without the need for transposing national law
- This should result in fewer divergences across EU Member States
  - However, Member State derogations will still exist in certain areas (e.g., employment)
General Data Protection Regulation (EU) 2016/679 (GDPR) – in a Nutshell

1. Extended Scope

2. Enhanced Individuals’ Rights

3. Explicit Accountability Requirements

4. Expanded Ex-EU Data Transfer Regime

5. Increased Enforcement & Fines
General Data Protection Regulation (EU) 2016/679 (GDPR) – in a Nutshell

1. **Extended Scope**

   - Material scope
     - New definitions
   - Territorial scope
     - Established in the EU
     - Not established in the EU
General Data Protection Regulation (EU) 2016/679 (GDPR) – in a Nutshell

2. Enhanced Individuals’ rights

• Right to be forgotten
• Right to data portability
• Right not to be subject to automated decision-making (profiling)
• Right to compensation
General Data Protection Regulation (EU) 2016/679 (GDPR) – in a Nutshell

3. **Explicit** Accountability Requirements

- Transparency (C)
- Recordkeeping (C+P)
- Privacy by Design/Default (C)
- Privacy Impact Assessments (C)
- Data Security (C+P)
- Data Protection Officer Designation (C+P)
- Vendor Relationships (C+P)
4. **Expanded Ex-EU Data Transfer Regime**

- Data “exports” still restricted under the GDPR
- Statutory duties for both controllers + processors when transferring personal data outside the EU
- Patchwork of solutions remains, but more options for transferring data
General Data Protection Regulation (EU) 2016/679 (GDPR) – in a Nutshell

5. Increased Enforcement & Fines

- Significant administrative fines for controllers + processors
  - Up to € 20 million / 4% of global turnover
  - To be determined on a case by case basis

- Cooperation mechanisms between Member State Supervisory Authorities
  - Lead to more coordinated + consistent enforcement?
Questions?

Contact:
Wim Nauwelaerts
Partner
Global Privacy & Cybersecurity Practice
Hunton & Williams
Brussels
+32 (0)2 643 58 00
wnauwelaerts@hunton.com
Borderless Cyber Europe
GDPR - what happens if it goes wrong
Breaches, remedies, liability and sanctions

**Aim**
To enhance the regulators’ and data subjects’ powers to hold controllers accountable and to ensure full and effective compensation of the person who suffered the damage as a result of the breach.

**Breach reporting**
- Controllers must inform the data protection authority of a breach without undue delay and, when feasible, within 72 hours after becoming aware of it.
- Requirement to document data breaches, including information about what happened, how it happened, the effect of the breach and any remedial action taken.
- Data subjects must be informed without undue delay if they are likely to be adversely affected by the breach.

**Enforcement**
- The data protection authority will have the power to order a controller to:
  - stop processing.
  - suspend data flows to a third party.
  - comply with a data subject’s request.
  - provide any information.
  - comply with prior authorisations.
  - rectify, erase or destroy personal data.

**Unlimited liability**
- Tougher enforcement regime and increased litigation risk means businesses are exposed to virtually unlimited financial liability.
- The data protection authority will have the power to issue fines of up to EUR20 million or 4% of annual worldwide turnover (whichever is higher).
- Data subjects have the right to bring court proceedings and class actions are envisaged for serious breaches.

**Business impact**
Data protection will be moved up the board’s agenda as an area of compliance, financial, litigation and reputational risk. Operational changes will need to be made to enable businesses to comply with the new breach reporting regime.

**GDPR reference**
- Article(s): 77, 82, 83
- Recital(s): 146
Cyber Security Directive – key requirement
Including breach reporting

Aim
Achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.

Focus areas
• Providers of essential services and digital services providers (energy, transport, FMI, health, water, DI, marketplace, search, Cloud)
• Member States to create CSIRTs, Competent Authority, SPOCs and national cooperation network
• MS to create national Strategy
• EU to create cooperation network
• Requirements to take appropriate technical and organisational measures for NIS

Enforcement
• Competent Authority has information access powers (policies, audit evidence and the like) and can issue “binding instructions” on ESP.
• For DSPs the powers are effectively the same.

Breach reporting
• Essential services providers to notify CA or CSIRT without undue delay, if significant incident (users affected, duration, geographical spread); CA/CSIRT to cascade to other MS, or to public.
• Digital service providers have same obligations, but tests are slightly different: they have to have enough information to make a decision on significance and significance test includes extent of disruption and economic/societal impacts

Business impact
Due to intersection of GDPR, ESPs and DSPs are now working under dual breach reporting and enforcement regimes. Those in the FS sector have more duties.
Privacy by Design

Ann Cavoukian
Executive Director of the Privacy and Big Data Institute, Ryerson University
Privacy Reference Model and Methodology (PMRM)

Gershon Janssen
Member OASIS PMRM Technical Committee
What is the PMRM?

A methodology and analytic tool developed to:

- enable the structured analysis of “use cases” in which personal information (PI) is used, generated, communicated, processed and stored
  - Support for applications, IoT, Cloud, complex hyper-connected systems, as well as smaller components of a system
- show the linkages among data, data flows, PI, privacy [including security] policies, privacy controls, privacy-enabling Services/functionality, and risk
- integrate with and support existing privacy standards
- achieve privacy by design requirements and compliance across policy and system boundaries
- support multiple stakeholders
Global Privacy Principles/Practices - similarities…but no Standardization

### OECD Guidelines – 1980
- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

### Australian Privacy Principles – 2001
- Collection
- Use and Disclosure
- Data Quality
- Data Security
- Openness
- Access and Correction
- Identifiers
- Anonymity
- Trans-border Data Flows
- Sensitive Information

### APEC Privacy Framework – 2005
- Preventing Harm
- Notice
- Collection Limitation
- Uses of Personal Information
- Choice
- Integrity of Personal Information
- Security Safeguard
- Access and Correction
- Accountability

---

from ISTPA “Analysis of Privacy Principles: An Operational Study” (2007)
GDPR – A Sampling of Rules Governing Processing of Personal Data

- Article 5 – Principles
- Article 6 – Lawfulness (including consent)
- Article 7 – Conditions of Consent
- Article 9 – Special Categories of personal data
- Chapter III – rights of data subject such as access, rectification, erasure, withdrawal of consent and data portability (Articles 16-18)

- Chapter IV - Obligations of Controller and Processor, including data protection by design and default, and
- implementation of mechanisms to demonstrate that processing is in compliance with the Regulation…etc.
PMRM v1.0 CS02 as “Model”
Multi-Stakeholder Implications
The PMRM Methodology

Privacy Management Analysis (PMA)

Use Case Description & High-Level Privacy Analysis
- Application and Business Process Descriptions
- Applicable Laws and Regulations
- Applicable Privacy Policies
- Initial Privacy Impact or Other Assessments

Detailed Privacy Analysis
- Participants and Systems
- Domains and Domain Owners
- Roles and Responsibilities
- Touch Points and Data Flows
- Incoming, Internally-Generated, and Outgoing PI
- Inherited, Internal, and Exported Privacy Controls

Services and Functionality Necessary to Support Privacy Controls
- Agreement
- Usage
- Validation
- Certification
- Enforcement
- Security
- Interaction
- Access

Operational Risk and/or Compliance Assessment

Technical and Procedural Mechanisms Supporting Selected Services

Implementation

Potential Privacy Architecture

PMRM Iteration
## PMRM Services

<table>
<thead>
<tr>
<th>Core Policy Services</th>
<th>Privacy Assurance Services</th>
<th>Presentation &amp; Lifecycle Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement</td>
<td>Validation</td>
<td>Interaction</td>
</tr>
<tr>
<td>Usage</td>
<td>Security</td>
<td>Enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access</td>
</tr>
</tbody>
</table>
Use Case

Emergency Responder Use Case: One Site Care
Use Case

Car Insurance – Reduction in Premiums

ACME Insurance Company
Toronto, Canada

Hudson Motor Company
Bruges, Belgium

Driving behaviour data:
- speed
- location
- trip frequency
- duration
- miles driven
- safety function deployment (e.g. ABS activation)

Calculate driving patterns related to driving behaviours and risk of accidents.

Increased reductions in premiums for driving patterns indicative of good driving behaviors and reduced accident risk.

Insurance Agent

Customer

Drivers

€
PMRM – Methodology

High Level Privacy Use Case Analysis

<table>
<thead>
<tr>
<th>Services/Applications</th>
<th>Privacy Requirements</th>
<th>Impact/Other Assessments</th>
</tr>
</thead>
</table>

Detailed Privacy Use Case Analysis

<table>
<thead>
<tr>
<th>Domains and Owners</th>
<th>Risks - Responsibilities</th>
<th>Data Flows and Touch Points</th>
<th>Systems [and Subsystems]</th>
<th>Actors</th>
</tr>
</thead>
</table>

PI in Use Case Systems

<table>
<thead>
<tr>
<th>System 1</th>
<th>System n</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Incoming/Internally Generated/Outgoing</td>
<td>Incoming/Internally Generated/Outgoing</td>
</tr>
</tbody>
</table>