Tackling the EU General Data Protection Regulation

For Research Organizations

Peter Milla peter@petermilla.com



www.cint.com



"Take aways" from this presentation:

Understanding of core requirements of the
EU General Data Protection Regulation (GDPR)

✓ The obligations of a research organization

✓ Practical tips and guidance for compliance

#WhoisCint

A global platform with multiple markets and considerations for data compliancy





1. Some Research

- 2. The GDPR
- 3. Practical Guidance



48% of UK adults plan to exercise rights under GDPR:

- **21%** of those in 45-54 year-old age group
- 13% of 18 -24 year-old age group

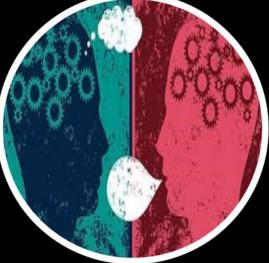
Most frequently mentioned rights:

- Right to access personal data (64%)
- Right to erasure (62%)
- Right to rectification (59%)



Some Research (continued)

- Confusion about what GDPR is
- Belief that it doesn't apply or may not go into effect in May, 2018
- Do not know which provisions apply
- Report that tracking changes are a challenge
- Lack of senior management awareness
- Concerns about requirements like breach notification
- Lack of budget





1. Some Research

2. The GDPR

3. Practical Guidance

EU Data Protection Framework

Directives:

- Individual implementation in each Member State
- EU Data Directive is a <u>directive</u>
- Sets a goal that a member state must achieve room for customization

Regulations:

- Immediately applicable in each Member State in a uniform manner
- Limited derogations permitted
- EU GDPR is a regulation
- Regulations are not negotiable by Member States

What is the GDPR?

The EU General Data Protection Regulation (GDPR):

- Officially known as Regulation (EU) 2016/679
- Replaces the EU Data Directive (Directive 95/46/EC)
- Is a **Regulation** (uniformly applicable in each member state)

Main Objectives:

- Give citizens back control of their Personal Data
- Simplify and unify regulation for business
- Applies to all member states in EU
- 'Data controllers', 'data processors' and 'sub processors'
- Addresses transfer of personal data outside the EU
- Significant fines (up to 20M EUR of 4% of revenue). US regulators will enforce.
- Goes into effect on **25 May 2018!**



Proposed ePrivacy Regulation

Replacement for existing ePrivacy Directive which regulates:

- Retention of Internet traffic
- Unsolicited email
- Cookies
- As a Regulation, it aims to consolidate member state implementation and align with the General Data Protection Regulation
- Penalties aligned with the GDPR



US

 With respect to data protection, viewed as not having adequate protections for data transfer from the EU



- Due to the differences in the regulatory models and practices. GDPR will be challenging for US companies:
 - Significant confusion, thinking that it doesn't apply
 - Lack of familiarity with concepts like subject access and data minimization
 - Concept of PII (vs. Personal Data in the EU context)
 - Issue for companies where the EU is a minority of their portfolio
- Impact of Facebook/Cambridge Analytica?

The Facts Include...

- 1. Applies to all operating in the EU
- 2. Revised definition of Personal Data
- 3. Privacy practices
- 4. Mandatory DPIAs
- 5. Rules for obtaining valid consent
- 6. Subject Access Rights, including the "Right to be forgotten"
- 7. Significant Fines/Liability (and Risk to Reputation)
- 8. Data Protection Officer
- 9. Information Security compliance
- 10. Data breach notification
- 11. Data Protection by Design
- 12. One-stop shop



What Will the EU Do?

- Initially will move cautiously (will react to complaints)
- Will look for evidence of compliance (in investigations)
- Based on past practice:
 - Expect that the EU will impose significant fines in time (tied to violation severity and size of entity)
 - Expect that US regulators will cooperate with EU authorities
- If a company is named in an action can face significant legal costs, large fines and reputational damage





- 1. Some Research
- 2. The GDPR
- 3. Practical Guidance

Data Transfer

- The US does not have adequate protections
- Existing mechanisms:
 - Model Contracts
 - Binding Corporate Rules
 - EU-US Privacy Shield (Positive first review)
 - Other alternatives exist under the regulation
- "Schrems 2.0":
 - Centers around the use of Model Contracts by Facebook as a "remedy" for "Schrems 1.0"

C A "Starters" Guide to Implementation

- 1. GDPR Data Protection Impact Analysis
- 2. Review Data Controller, Data Processor and Sub Processor Status
- 3. Appoint a Data Protection Officer (DPO)
- 4. Review privacy policies and T&Cs
- 5. Address data transfer requirements
- 6. Address Data Subject Access (SARs) requests
- 7. Review Contracts (Subcontractors, Clients, etc.)
- 8. Review/Develop Breach Notification Policy/Process

GDPR is About Good Practices

- Take a **holistic** and automated approach to governance and compliance
- Be **structured** about the data you collect:
 - Knowing what you can/cannot use
 - Managing and understanding data lineage
- Make sure you properly address consent
- Data "hygiene":
 - Data collected and processed in an "above board" manner
 - Transparency



GDPR as a Baseline for Compliance

- Many companies face global compliance requirements beyond the EU and GDPR (China, Japan, Russia, US, etc.)
- GDPR extends the compliance requirements included in the EU Data Directive. The Directive was a basis for other regulation like the PIPEDA in Canada and the Australian Privacy Act.
- Requirements seen in GDPR have commonality. This is true for HIPPA.
- Framework for operation and growth that can be applied to the US

C Useful Links

- Cloud Industry Forum: <u>www.cloudindustryforum.org</u>
- EU GDPR Portal: <u>http://www.eugdpr.org/more-resources-1.html</u>
- EU Commission GDPR Page:<u>http://ec.europa.eu/justice/data-protection/reform/index_en.htm</u>
- Article 29 Working Party: <u>http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083</u>
- EU Data Protection Authorities: <u>http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm</u>
- UK Data Protection Authority: <u>https://ico.org.uk/</u>
- German Data Protection Authorities: <u>https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Daten</u> <u>schutzbeauftragte/Datenschutzbeauftragte.php</u>

Tackling the EU General Data Protection Regulation

For Research Organizations

Peter Milla peter@petermilla.com



www.cint.com