RSA Conference

Where the world talks security

Breach Notification in the GDPR Era

Speakers:

Sam Pfeifle, IAPP
Dennis Holmes, PwC

Welcome

Sam Pfeifle,
Content Director,
IAPP
sam@iapp.org

Dennis Holmes, Lawyer,
Cybersecurity and Data Protection Legal Services,
PwC UK
dennis.holmes@pwc.com

GDPR's Security Requirements

- Must ensure "appropriate security and confidentiality of the personal data"
  - Must evaluate risks, then takes steps to mitigate those risks
  - Security should be both "technical" and "organizational"
  - Mitigation considers "state of the art" as well as cost
  - Must also protect against destruction, not just access
  - Need a demonstrable process for testing security's efficacy
  - Codes of conduct or certification can stand for documentation
  - Controller is responsible for processor's security

GDPR's Breach Notification Requirements

- What's the trigger?
  - Personal data breach
    - Destruction, Loss, Alteration, Disclosure, Access
  - But not if the breach is unlikely to result in risk to rights and freedoms
  - Processor just has to notify the controller, then controller notifies further

- Must notify the DPA within 72 hours of becoming "aware"
  - If more than 72 hours, you need a "reasoned justification"

GDPR's Breach Notification Requirements

- What's in the notification?
  - Nature of the breach, including how many records and data subjects
  - DPO's contact information
  - Likely consequences of the breach
  - How the controller will address the breach, mitigation efforts

- If breach is likely to result in a "high risk" to data subjects, notify them as well, unless:
  - Controller put in tech controls to make data unintelligible
  - Controller did something to make high risk "unlikely"
  - Notification would require "undue effort"

With which is it most risky not to comply?

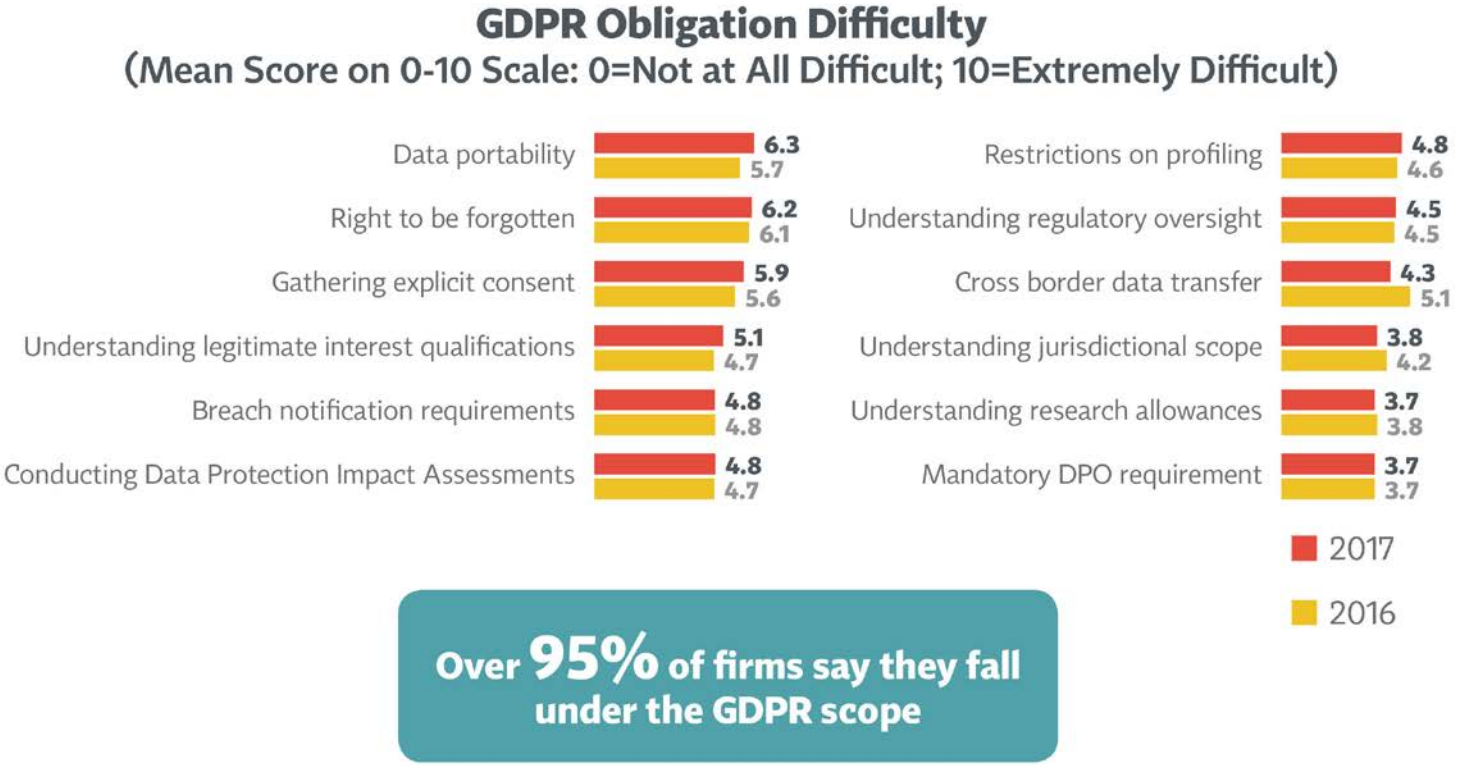
- Operationalizing the right to be forgotten.
- Operationalizing data portability.
- Obtaining/managing user consent.
- Complying with international data transfer requirements.
- Preparing for data breach notification.
- Conducting data protection impact assessments.
- Establishing legitimate interest for data processing.
- Conducting data inventory/mapping.
- Maintaining records of processing (e.g. Article 30 reports).
- Managing data subject requests.
- Appointing a data protection officer (DPO).

With which is it most risky not to comply?

How Risky Is Non-Compliance With the Following GDPR Obligations
(Scale Of 1-5, With 1 Being "No Risk" And 5 Being "High Risk")

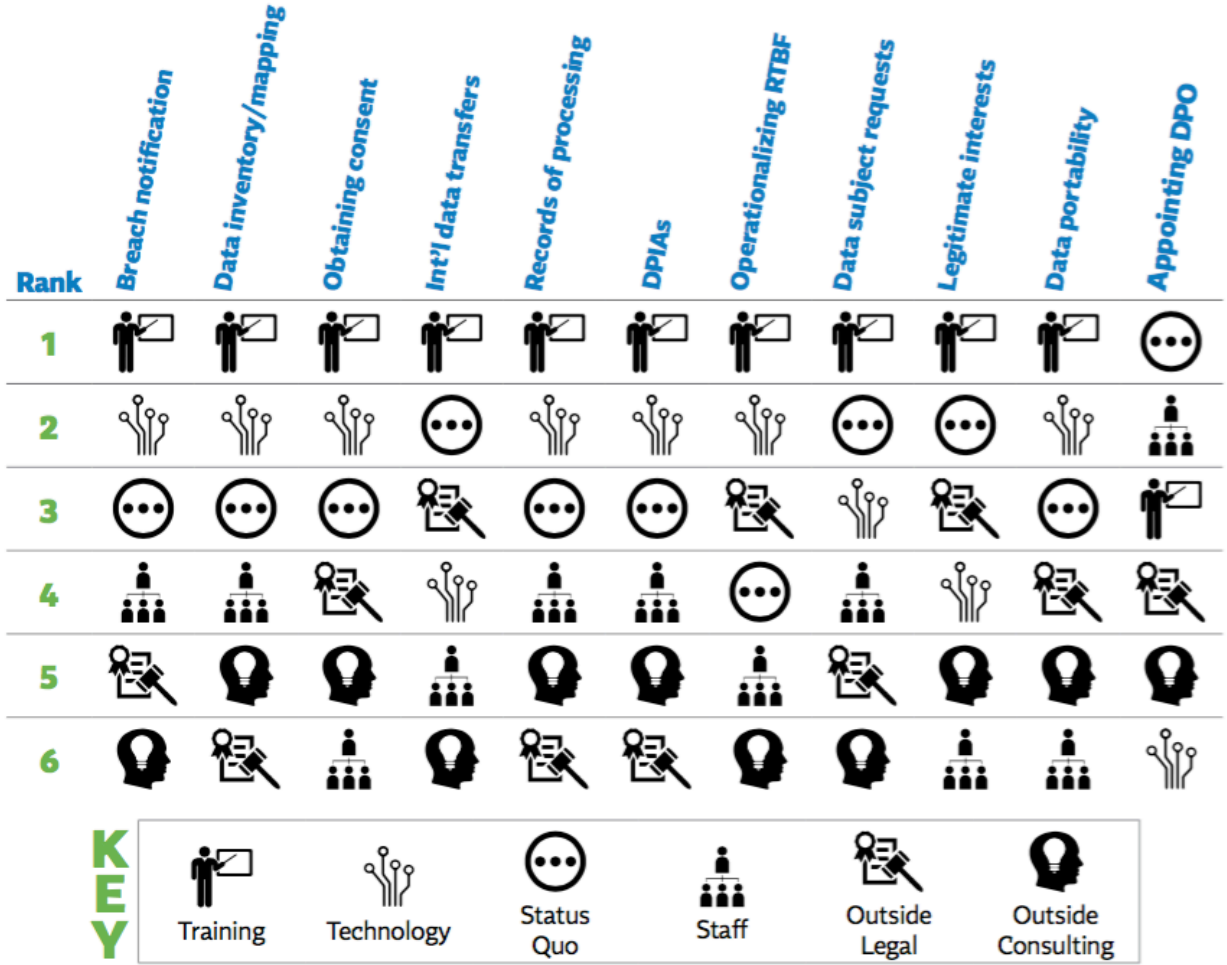
Overall		U.S.		EU	
Prep. for breach	3.66	Int'l data transfers	3.76	Prep. for breach	3.68
Data inventory/mapping	3.57	Obtaining consent	3.61	Data inventory/mapping	3.57
Obtaining consent	3.54	Prep. for breach	3.6	Maintain. Art. 30 records	3.51
Int'l data transfers	3.54	Data inventory/mapping	3.6	Obtaining consent	3.44
Maintain Art. 30 records	3.48	Maintain Art. 30 records	3.42	Conducting DPIAs	3.35
Conducting DPIAs	3.36	Data subject requests	3.37	Int'l data transfers	3.31
Operationalizing RTBF	3.34	Conducting DPIAs	3.33	Data subject requests	3.3
Data subject requests	3.34	Operationalizing RTBF	3.26	Operationalizing RTBF	3.21
Establish legit interest	3.14	Establish legit interest	3.18	Establish legit interest	3.08
Data portability	2.88	Data portability	2.92	Appoint DPO	2.85
Appoint DPO	2.87	Appoint DPO	2.9	Data portability	2.79

Compare that to perceived difficulty…



How will you mitigate that risk?

- Investing in privacy/data protection training.
- Increasing number of privacy staff.
- Investing in additional outside legal assistance.
- Investing in additional outside consulting assistance.
- Investing in privacy/data protection technology.
- Continuing the status quo privacy program.



How will you mitigate that risk?

RSA Conference

How To Prepare for a Breach

The people you need on your team

Legal Services: Really a breach? Have to notify?

- What is a risk to rights and freedoms?
- What is a high risk to rights and freedoms?
- Do you have a DPO?
- Is your DPO a lawyer?
- In how many jurisdictions do your data subjects reside?
- Who's your regulator?

Forensics: What actually happened?

- When do you become aware?
- Which of the triggers actually happened?
- What was the nature of the data accessed?

Public Relations: What does notification look like?

- Who crafts the message?
- Who gets which message?
- Who speaks for the organization?
- How is the brand impacted?

Consumer Services: Making it good

- Identity theft monitoring?
- Credit monitoring?
- What makes sense in which jurisdiction?
- Actual reparations?

Questions?

Sam Pfeifle,
Content Director,
IAPP
sam@iapp.org

Dennis Holmes, Lawyer,
Cybersecurity and Data
Protection Legal Services,
PwC UK
dennis.holmes@pwc.com