May 25th Came and Went – Now What Do You Do?

Gary Sheehan

ASMGi

August 23, 2018

Triad ISSA Meeting

gsheehan@asmgi.com

ASMGi™

- CSO / Director of GRC Services
- 30 years in Information Security
- GRC / IS Program Development
- Broad background in Security

INFORMATION SECURITY SUMMIT℠
Building Community Through Education

CAREER CONNECTION

CSOXchange

INFORMATION SECURITY SUMMIT
Confidentiality | Integrity | Availability

- Non-profit – 2002 - Mission
- Volunteer organization
- Events / Education / Networking
- **The *SUMMIT* 2018**
- Unique business model
- Exciting announcement!

Abstract

On May 25, 2018 organizations with business ties to the European Union needed to comply to GDPR standards or face fines. Many U.S.-based companies falsely believe that they cannot be impacted by GDPR because they don't have a European office or customers in Europe. ***In reality, any company that has customers living in the U.S. with European citizenship or partners or visitors to their website from Europe need to comply with GDPR.***

In this session we will:

- Review the GDPR hot buttons
- Review what has happened in the GDPR world since May 25th
- Discuss the path forward – what can/should you do today

Definition

GDPR is short for General Data Protection Regulation, and it's the name of a law in the European Union (EU) that sets out to protect the rights of individuals in respect of their data.

The General Data Protection Regulation (GDPR) was adopted by the EU in April 2016 and replaced the EU Data Protection Directive 95/46/EC. The GDPR introduces new obligations to data processors and data controllers, including those based outside the EU.

Loosely speaking, **any organization** that holds data or information about any resident of the EU is expected to comply.

GDPR Hot Buttons

- The GDPR focuses on accountability, transparency and governance.
- Many of the GDPR requirements are specific processes organizations must adopt.
- Hefty fines.
- Vague Requirements - GDPR does not articulate a precise prescription for the technology
- Extraterritorial Reach

GDPR Hot Buttons

- What We Know For Sure:
  - GDPR takes a risk-based approach to requiring particular technical measures.
  - GDPR is supported with enforcement mechanisms, and those mechanisms far exceed what has been in place until now.
  - Class Action Suits – Collective Proceedings
  - Undertaking meaningful steps toward comprehensive security compliance demonstrates to courts and regulators that an organization is a responsible steward of data and potentially worthy of lenient treatment

GDPR Hot Buttons

- Who has the responsibility?
  - Organizational Structure
  - Data Breach, Collection, Protection and Use
  - Managing Consent
  - Privacy Notice
  - Risk Management
  - Third-Party Data Use
  - Anonymizing collected data to protect privacy
  - Providing data breach notifications
  - Safely handling the transfer of data across borders

GDPR Hot Buttons

The paramount question the GDPR poses to security practitioners is not ***"What checklist of measures must I follow to pass an audit?"*** Instead, the paramount question is:

How do we avoid a breach and how do we return control of PII back to the consumer?

What's Happened?

- Several high-profile US news sites (ie: LA Times, New York Daily News, Chicago Tribune, Baltimore Sun, etc.) have been blocked to European users
- Medical Treatment Cancelled - Duchy Hospital in Truro said it took patients' confidentiality seriously and, as a result of the new GDPR regulations which came into effect at the end of May, it had been necessary to undertake some additional compliance checks with third-party companies currently based outside the EU.

What's Happened?

Enforcement Action – 189 Actions Taken so far.

- 100 Monetary Penalties
- 36 Enforcement Notices (ICO Order for compliance)
- 27 Undertakings (Signed agreement to comply)
- 26 Prosecutions (Most all were prosecuted for failing to comply with the Data Protection Act of 1998 – but were brought to the Information Commissioner's Office under GDPR.)

What's Happened?

- The UK Information Commissioner's Office (ICO) has provided Facebook with a Notice of Intent to issue a monetary penalty against the social media platform for its lack of transparency and failure to maintain the security of its users' personal data in relation to the Cambridge Analytica scandal. (breaches of the first and seventh data protection principles under the Data Protection Act 1998.) The ICO's Notice of Intent provides for a fine of £500,000 ($665,000) which is the maximum fine that the ICO can levy under the Data Protection 1998. Facebook's infringing activity occurred prior to the EU data protection regime under the General Data Protection Regulation (GDPR) coming into full effect.

The Path Forward

ICO Website

The Path Forward

WHAT YOU NEED TO DO:

- Adopt a security framework
- Create a Written Information Security Program (WISP)
- Utilize emerging guidance on key provisions – Get legal advice
- Watch out for inconsistencies between E.U. member states.
- Monitor third-party vendors.
- Understand the GDPR's breach notification clauses—and similar U.S. notification requirements.
- Recognize your regulatory and litigation risks.
- Consider whether existing insurance policies provide appropriate coverage.

The Path Forward

WHAT YOU NEED TO KNOW:

- GDPR is a Global Law – It is an Issue
- You need more than a registered agent or ‘EU Representative’ and an official address within an EU member country to show compliance
- GDPR applies to digital and hardcopy data
- Your DPO must be qualified
- Understand what constitutes “Personal Data”
- There is no such thing as “GDPR Compliant”
- EVERYONE is a target, big and small
- Fines are NOT limited

Summary

- Review the GDPR hot buttons
- Review what has happened in the GDPR world over the last 90 days
- Discuss what companies can/should do moving forward.

According to The Ernst & Young 2018 Global Forensic Data Analytics Survey, only 13% of the Americas respondents indicated they have a GDPR Plan in place

GDPR's primary principle is that personal data is the property of the individual, not data controllers or processors. It applies to all EU citizens wherever they may be situated and regardless of the organization's location.


Q
&
A