PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

Sword vs. Shield: Using Forensics Pre-Breach in a GDPR World

September 20, 2017

Presented by PLUS Diamond Sponsors

AXIS beazley CNA We can show you more. SOMPO INTERNATIONAL HISCOX encourage courage TRAVELERS

PLUS

The information and opinions expressed by our panelists today are their own, and do not necessarily represent the views of their employers or of PLUS. The contents of these materials may not be relied upon as legal advice.

A copy of the presentation slides will be available following this webinar, on the PLUS website at: www.plusweb.org

Meet The Presenters

Winston Krone
Global Managing Director, Amsterdam Office
Kivu Consulting

Cinthia Granados Motley
Partner, Chair Data Privacy & Security Practice
Sedgwick LLP

Kim Holmes
SVP, Counsel, Cyber Insurance, Liability & Emerging Risks
ID Experts

Agenda

- GDPR - BRIEF OVERVIEW
- IF YOUR ORGANIZATION IS SUBJECT TO GDPR…
- PREPARING FOR GDPR: ARE CURRENT PRACTICES COMPLIANT?
- USING FORENSICS PRE-BREACH TO PREPARE FOR GDPR
- ATTORNEY-CLIENT PRIVILEGE
- BEST PRACTICES TO CONSIDER

PLUS

GDPR:
(General Data Protection Regulation)

Brief Overview

Key Concepts

- Strict global privacy requirements *standardizing* how personal data of EU citizens is processed, managed and stored, in tandem with individuals' choice – wherever personal data is managed, sent, processed or stored
- Transparency required re: handling and use of personal data
- Limitations as to specific, legitimate purposes
  - Data processing

Key Concepts

- Limitations to intended purposes
  - (i.e., storage and data collection: only as long as needed for intended purpose)
- Individuals' right to correct/request erasure (deletion) of their personal data
- Appropriate security practices required
- Significant potential fines for non-compliance
  - Up to 4% of global Net Revenue for willful violations

- **APPLICABLE TO WHOM?**
  - Organizations with an “establishment” in the EU regardless of where they process personal data.
  - Organizations based outside the EU that provide services or goods to the EU (different than before).
  - Organization offering goods and services to EU citizens or that collect, store, or analyze data on EU citizens – no matter where they are in the world.

- **APPLICABLE TO WHAT?**
  - Personal Data –"any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."
  - Sensitive Personal Data ("SPD")- genetic and biometric data

Personally Identifiable Information

- An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information.

- Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

PLUS

If Your Organization is Subject To GDPR…

GDPR: Individual Rights

- Individual data subjects' rights:
  - to know if organization is processing their data;
  - to understand purpose of same;
  - to have data deleted/corrected or ask to have processing stopped;
  - to object to direct marketing;
  - to revoke consent for certain uses of their data;
  - to portability (moving their data and assistance from organization in doing so)

Notification Requirements

- **WHO** must be notified?
  - Data Privacy Authority (DPA)
  - Supervisory Authority (SA)
  - Role of Data Privacy Officer (DPO)

- **WHEN** must notification occur?
  - No longer than 72 hours from discovery
  - Unless unlikely to result in a risk

Notification Requirements

- Notification must include:
  - Categories and approximate number of individuals affected – identify users, their relationship to organization (customers, business partners, employees, etc.)?
  - Categories and approximate number of personal data records concerned
  - Question: how “approximate” will regulators want?

Notification Requirements

- Description of likely consequences of personal data breach – akin to US “likelihood of harm” analysis

- Description of mitigation/remediation efforts
  - What has been done, or what will be done to mitigate the personal data breach and/or to reduce the potential impact of the breach

Other Specific Requirements

- Data protection/impact assessments
  - Predicting privacy impact of projects and efforts to mitigate risk
- Records maintenance
  - All processing activities, consents to data processing, compliance with GDPR
- Legal basis for processing personal data
  - Individuals' consent must be "freely given, specific, informed and unambiguous"

PLUS

Preparing for GDPR: Are Current Practices Compliant?

Are You GDPR-Compliant Today?

- Mapping Sensitive Information
- Implementing a Data Diet
- Evaluating Maximum Probable Loss Based on Number of Records
- Determining Adequacy of Organization's Insurance
- Ensuring Vendors Have Adequate Cyber Insurance for Data
- Updating AND TESTING Incident Response Plan
- Addressing Vendor/Business Partner Cyber Hygiene Beyond Warranties/Indemnification Agreements
- Considering M&A Issues

PLUS

Using Forensics to Prepare for GDPR

The Good News…

- Most of the GDPR notification requirements above are already relevant to US forensic breach investigations.
- With pre-emptive planning, an organization can set up its auditing and logging capabilities to specifically address many of these requirements and assist with the forensic investigation - critically important given the time constraints to carry out the investigation under GDPR.
- As in the US, the ultimate cost of forensics is often more dependent on the pre-breach measures adopted by the organization (e.g. the amount of logging, auditing) and less to number of records affected.

The Bad News…

- In the US, forensics is usually phased with much of the granular analysis (determining exactly whose data was taken and the likely impact) only AFTER certain thresh-holds have been triggered.

- Years of experience allows us to know what specific state/Federal regulators expect in terms of the forensics investigation.

- In the US, this allows for a phased approach, triaging expenditure over time – with some forensic analysis ultimately deemed to be not necessary.

The Bad News…

- In the EU, the upfront investigations may need to be more detailed/wider than US and EU regulators will (at least in the first year?) seek answers to all the above questions.

- Insurers should be ready for the forensics phase to be larger than comparable US breaches, at least until guidance is obtained from the EU regulators as to what they will be expecting.

PLUS

Attorney-Client Privilege: Be Mindful

ATTORNEY-CLIENT PRIVILEGE

- Cybersecurity consultants' work product and communications
  - Like that of other retained experts – are subject to confidentiality under the attorney-client privilege and/or the work product doctrine when counsel retains the consultants for the purpose of obtaining technical assistance to enable counsel to render legal advice to a client
- Validates the decision by organizations to designate legal counsel as the lead in key cybersecurity activities, such as scoping and directing proactive security risk assessments and directing reactive forensic investigations and response efforts following a data breach

PLUS

Thinking About GDPR-Prep Best Practices Going Forward...

GDPR PREP: BEST PRACTICES

- Revise your incident response plan to allow for a possible 72 hour notification
- Design your cyber defenses not only to keep hackers out but, in the case of an intrusion, to explain what hackers did
- Establish clear and sound policies that meet the data protection standards of adequacy required by GDPR
- Establish privacy by design- conscious, considered policies and implementation to comply and respect data privacy
- Analyze legal basis on which data processing is provided- is your basis documented?

GDPR PREP: BEST PRACTICES

- Have established security breach processes and policies
- BREACH NOTIFICATION is required if risk to rights and freedoms of data subjects exists. (within 72 hours of discovery)
- Make sure privacy notices and policies are clear and in plain language, understandable to all affected
- Review disclosure about CONSENT to make sure it is explicit for SPD.
  ENSURE CONSENT is understood to be freely given by data subjects - not coerced (CLICKWRAP AGREEMENTS)
- Be knowledgeable & able to respond to data subjects
- Respect rights of data subjects
- Ensure: (1) organization's clients are aware of new compliance with Regulation and (2) Data Processors understand their role

PLUS

Questions?

Please submit using the question tool on user dashboard

Thank You Presenters

Winston Krone
Global Managing Director, Amsterdam Office
KIVU Forensic Consulting

Cinthia Granados Motley
Partner, Chair Data Privacy & Security Practice
Sedgwick LLP

Kim Holmes
SVP, Counsel,Cyber Insurance, Liability & Emerging Risks
ID Experts

PLUS

Presented by PLUS Diamond Sponsors

PLUS

Thank you for your time.

A replay of this webinar will be available to PLUS Members at:
www.plusweb.org