GDPR is coming soon. Are you ready.

Steven Ringelberg

steven@ringelberglaw.com

616 227 6403

Agenda

- Who am I
- Overview
- What data do you have that is covered and where is it?
- What rights do individual data subjects have?
- Data breach response.

STEVEN RINGELBERG

- Managing Partner, Ringelberg Law LLP, Washington, D.C.
- Data privacy, cybersecurity and intellectual property law, regulations and policies.
- Former Chief Executive Officer, Vanguard Integrity Professionals, 2007 to 2015.
- Former in-house counsel for Vanguard, Exstream Software, Honkworm, Baan Software, and Microsoft.
- JD, New York University School of Law, BA, Oberlin College.

EU GDPR OVERVIEW

- **General Data Protection Regulation enacted in May 2016, effective May 25, 2018.**
- **Regulation (EU) 2016/679.**
- **Replaces the EU Data Privacy Directive from 1995.**
  - Data Privacy Directive was implemented by statute in each of the EU countries over the following years.
  - Each implementation in each country was slightly different or very different.
  - Each country had jurisdiction over any company that was located within their borders, or had data on residents within those borders.
  - Lots and lots of regulatory overlap, very little guidance on implementation of effective data security.

EU GDPR OVERVIEW

Your choice:

1. Do not collect or process data on European Union Residents.

Possible, but may negatively impact your business.

2. Fully Comply with GDPR.

Expensive.

3. Ignore It.

Risky.

EU GDPR OVERVIEW

- Single Regulation.
- Does not need implementation of a country by country basis.
- Replaces the individual country implementations.
- With one law on data protection across all 28 member states, organizations no longer have to manage different data protection approaches per market. The European
- European Commission estimates this will save businesses around €2.3 billion annually.
- Provides more granular guidance on data security requirements.
- Provides for a single regulatory authority to have oversight of all companies based within their borders.
- Increases the rights of individual data subjects.
- Increases that penalties for data breaches

EU GDPR OVERVIEW

- The GDPR defines two important roles – that of “controller” and “processor” – and your organization may fall under either one or both of these definitions. A “controller” alone or jointly with others, determines the purposes and means of the processing of personal data whether on-premises or while using a third-party cloud provider’s IT technology, whereas a “processor” processes personal data on behalf of a controller.

- While an organization cannot be both a controller and a processor of the same data, it is possible for an organization to be a controller of one set of data and a processor of yet another.

EU GDPR OVERVIEW

- Complying with the GDPR requires both organizational and technological measures in response.
- Organizational measures include appointing a Data Protection Officer, policies and training on handling personal and sensitive personal data, and an approach for executing a Data Protection Impact Assessment (DPIA).
- Technological measures for protecting personal or sensitive personal data include data classification, data loss prevention, encryption, managing consent more explicitly, data transfer limitations, and technologies that enable data subjects to exercise their rights to access, rectify, and erase personal data held by data controllers (subject to certain conditions).

- The GDPR is focused on the *protection* of personal data, not merely the *privacy* of personal data. Complying with the protection mandate requires a higher degree of proactive and far-reaching effort on the behalf of organizations that process personal data.

EU GDPR OVERVIEW

Article 24 sets the general obligations for a data controller: “the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”

EU GDPR OVERVIEW

Article 28 sets the general obligations for data processors: data processors must “implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”

EU GDPR OVERVIEW

The right to process personal data must be lawful, with six categories of lawfulness listed in Article 6, the first of which is that the data subject has “given consent to the processing ... for one or more specific purposes.” Other lawful bases include contract performance, compliance with a legal obligation, and protection of the vital interests of the data subject.

EU GDPR OVERVIEW

- Article 30 requires that controllers “shall maintain a record of processing activities under its responsibility,” and lists seven types of information to be maintained, including the purpose of the processing, a description of categories of data subjects and personal data, and who will see the personal data after processing, among others.
- Processors have a similar requirement to record all categories of processing activities. Both controllers and processors are required to keep these records in written form, with electronic form permitted under Article 30.

EU GDPR OVERVIEW

Organizations are required to appoint a data protection officer if processing of personal data and/or sensitive personal data is regular and systematic (Article 37), although there are various forms the appointment can take on account of organizational type and size.

The data protection officer requires “expert knowledge of data protection law and practices” (Article 37(5)), must have certain freedoms (Article 38), and has a list of prescribed tasks to execute (Article 39).

These tasks include informing and advising data controllers, processors, and employees of their obligations under the GDPR, monitoring internal compliance, and cooperating with the supervisory authority, among others.

WHAT DATA DO YOU HAVE THAT IS COVERED AND WHERE IS IT?

- The GDPR imposes rules on organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where those businesses are located.

WHAT DATA DO YOU HAVE THAT IS COVERED AND WHERE IS IT?

- GDPR covers any information related to an identified or identifiable natural person.
- That can include both direct identification (e.g., your legal name) and indirect identification (i.e., specific information that makes it clear it is you the data references).
- GDPR includes online identifiers (e.g., IP addresses, mobile device IDs) and location data where the EU Data Protection Directive had previously been somewhat unclear.

WHAT DATA DO YOU HAVE THAT IS COVERED AND WHERE IS IT?

- The GDPR introduces specific definitions for genetic data (e.g., an individual's gene sequence) and biometric data. Genetic data and biometric data along with other sub categories of personal data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; data concerning health; or data concerning a person's sex life or sexual orientation) are treated as sensitive personal data under the GDPR. Sensitive personal data is afforded enhanced protections and generally requires an individual's explicit consent where these data are to be processed.

WHAT DATA DO YOU HAVE THAT IS COVERED AND WHERE IS IT?

- The GDPR has elevated protection for special categories of personal data.
- Article 9(1) states the general prohibition as such: “Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.” Article 9(2) then lists ten separate exclusions to this general prohibition, including consent from the data subject, the protection of vital interests of the data subject, and where the data subject has made such information public, among others.

WHAT DATA DO YOU HAVE THAT IS COVERED AND WHERE IS IT?

Articles 44-50. Transfers of Personal Data to Third Countries or International Organizations

The GDPR outlines specific requirements governing when and where personal data can be transferred to third countries or international organizations. While Safe Harbor was determined to be invalid in late 2015, it was replaced by the EU-US Privacy Shield framework as of mid-2016. The goal of the framework is to permit US companies to transfer data on EU residents while still maintaining the protections afforded under the GDPR.

- But See: Microsoft v. United States, currently before the U.S. Supreme Court. **Articles 44-50. Transfers of Personal Data to Third Countries or**
- **International Organizations**
- The GDPR outlines specific requirements governing when and where personal data can be transferred to third countries or international organizations. While Safe Harbor was determined to be invalid in late 2015, it was replaced by the EU-US Privacy Shield framework as of mid-2016. The goal of the framework is to permit US companies to transfer data on EU residents while still maintaining the
- protections afforded under the GDPR.

WHAT RIGHTS DO INDIVIDUAL DATA SUBJECTS HAVE?

- **Enhanced personal privacy rights:** strengthened data protection for residents of the EU by ensuring that they have the right to access their personal data, to correct inaccuracies in that data, to erase that data, to object to processing of their personal data,and to move it.

WHAT RIGHTS DO INDIVIDUAL DATA SUBJECTS HAVE?

- **Article 15. Right of Access by the Data Subject**

A data subject has the right to ask a data controller whether his or her personal data is being processed, and if so, can request access to both the personal data and information on processing, recipients, data transfers, and subsequent rights (such as the right to complain to a supervisory authority, or the right to request rectification, erasure, or a restriction on future processing). Data subjects have the right to know if and when their data is transferred to a third country or an international organization, along with the safeguards in place to ensure ongoing protection of the data after transfer. A data controller must provide a copy of any personal data undergoing processing at no charge the first time it is requested, but has the right to charge “a reasonable fee based on administrative costs” for subsequent requests.

WHAT RIGHTS DO INDIVIDUAL DATA SUBJECTS HAVE?

Article 16. Right to Rectification

If a data controller holds inaccurate personal data about a data subject, the data subject has the right to supply the correct information to get their personal data updated. The data controller is required to rectify the inaccurate information "without undue delay."

WHAT RIGHTS DO INDIVIDUAL DATA SUBJECTS HAVE?

Article 16. Right to Rectification

If a data controller holds inaccurate personal data about a data subject, the data subject has the right to supply the correct information to get their personal data updated. The data controller is required to rectify the inaccurate information "without undue delay."

WHAT RIGHTS DO INDIVIDUAL DATA SUBJECTS HAVE?

Article 17. Right to Erasure (Right to be Forgotten)

Subject to certain conditions, a data subject has the right to request the erasure of his or her personal data held by a data controller. Conditions include the withdrawal of consent, previous unlawful processing, and other legal compliance erasure mandates.

Data controllers, on the other hand, have the ability under the GDPR to decline an erasure request if it falls within one of the several exclusions in Article 17(3), such as compliance with a legal obligation, public interest for public health, and legal claims. Nonetheless this requires that organizations have a very clear legal understanding of why they are processing data, the appropriate legal bases and when required, a technological ability to erase all affected data promptly.

WHAT RIGHTS DO INDIVIDUAL DATA SUBJECTS HAVE?

Article 18. Right to Restriction of Processing

Article 19. Notification Obligation for Controllers

Article 21. Right to Object

DATA BREACH RESPONSE.

- **Mandatory personal data breach reporting:** organizations that control personal data are subject to stringent reporting and notification requirements in the event of a personal data breach.
- **NOTIFICATION OF DATA BREACHES TO THE RELEVANT SUPERVISORY AGENCY WITHIN 72 HOURS.**

DATA BREACH RESPONSE.

Article 33(3) specifies four requirements insuch a notification:

The nature of the personal data breach (including categories of data and approximate number of data subjects impacted).

The name and contact details of the firm's data protection officer.

An analysis of the likely consequences of the breach.

Measures taken or proposed to be taken to mitigate negative effects.

The exemption to these requirements is where “the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons,” by for example, having the data encrypted.

DATA BREACH RESPONSE.

The second requirement is to notify data subjects individually of any personal data breach that has a high risk to their individual rights and freedoms (Article 34), and must contain similar information to that notified to the supervisory authority. There are some exemptions and exceptions noted in Article 34(3), such as if the organization had “appropriate technical and organizational measures” (e.g. encryption) in place to protect the data.

GDPR PENALTIES

Significant penalties for non-compliance:

Large sanctions, including substantial fines that are applicable whether an organization has intentionally or inadvertently failed to comply.

Financial penalties of up to a €20 million fine or 4% of total worldwide annual turnover of the preceding financial year, whichever is higher.

GDPR PENALTIES

In ascertaining the amount of any fine to apply, Article 83 of the GDPR makes clear
the intent is that it should “be effective, proportionate and dissuasive.”

Any fine must be calculated in light of multiple factors, including the nature, gravity and duration of the infringement; the presence of negligence, organizational and technological mitigations in place; the categories of personal data affected; and whether the organization itself notified the supervisory authority of the infringement.

GDPR PENALTIES

- **Article 83(2) lists 11 separate factors for a supervisory authority to evaluate when setting the level of the fine, with Articles 83(4) and 83(5) specifying the types of infringements that fall into the two-percent and four-percent regimes, with infringements on the basic principles for processing, data subjects' rights, and transfers of personal data falling under the higher fine regime.**
- **The four percent/€20 million fines also relate to Article58(2), whereby the controller/processor is non-compliant with an order by the supervisory authority.**