Data Privacy, Protection and Compliance From the U.S. to Europe and Beyond

InsideNGO's 2017 Annual Conference
Washington, DC
July 20, 2017

Shannon Yavorsky – Partner, Venable LLP

David Goodman – Global Non-Profit CIO

VENABLE LLP

Questions

I. How many of you believe you understand and have the issues of data protection and info sec well in hand?

I. How many of you have budget and headcount for data protection and info sec?

II. How many of you understand if and how GDPR will affect your organization?

What We Will Cover

I. What is GDPR?

II. How might it affect my organization?

III. What should I do??

Privacy v. Data Security

- Privacy – Focused on rules governing deliberate acts of "pushing" personal information out of an organization, typically in connection with acquiring or retaining customers
  - For example: renting of customer lists or sharing of customer information with corporate affiliates

- Data Security – Focused on rules aimed at protecting personal information from being "pulled" out of an organization
  - For example: external hacking or theft by an employee

- Europeans collapse both concepts under the rubric of "data protection"

Privacy Terminology: Other Key Terms

- **Data Controller** – the entity which determines the purpose and means of the processing of personal data.
- **Data Processor** – the entity which processes personal data on behalf of the controller.
- **Consent** –
  - **EU** – any freely given, specific, informed and unambiguous indication of a data subject's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to the data being processed.
  - **US** – consent can be provided where a person does not opt-out of a company's stated information practices after receiving notice, or, where sensitive data is involved, consent may be given by opting-into specified information practices.
- **Anonymous Data** – data that does not permit the re-identification of individuals.
- **Pseudonymous Data** – data from which individuals can be identified using a key.

The General Data Protection Regulation

- **Countdown.** The GDPR will apply in all Member States from May 25, 2018.

- **Territorial Scope.** The GDPR expressly applies to any processing of personal data of data subjects in the EU regardless of the company's location.
  - Non-EU established organizations who:
    - Offer goods and services to EU data subjects; or
    - Monitor the behavior of EU data subjects.
  - Non-EU organizations will need to appoint a representative in the EU unless it meets certain requirements that reduce the risk to EU citizens.

The General Data Protection Regulation

- **Penalties.** Regulators can impose fines up to 4% of worldwide turnover or 20 Million euros (whichever is higher).

- **Accountability.** What's your compliance story?

GDPR Core Concepts - Definitions

Definitions.

- Expanded definition of “personal data”.
  - Includes cookies, device IDs, and other online identifiers.
  - Expanded definition of sensitive personal data now includes genetic data and biometric data.
- Strengthened definition of “consent.”
  - Consent must be freely given, specific, informed and unambiguous.
  - Individuals must have the right to revoke consent.
  - There is a presumption that consent will not be valid unless separate consents are obtained for different processing activities, general, omnibus consent will not be valid.

GDPR Core Concepts – Lawful Basis for Processing

What is your lawful basis for processing?

- Consent of the data subject.
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
- Processing is necessary for compliance with a legal obligation.
- Processing is necessary to protect the vital interests of a data subject or another person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

GDPR Core Concepts – Rights of Data Subjects

- **Right to be forgotten.**
  - Personal data must be erased without undue delay when:
    - Retention is not required.
    - Data is no longer needed.
    - Consent has been withdrawn.
- **Data portability.**
  - Individuals must be given the right to transfer data to another service provider where technically feasible.

GDPR Core Concepts – Rights of Data Subjects

- **Right to be informed.**
  - Privacy Notices.
  - Transparency about how data is used.
- **Right of access.**
  - Individuals are entitled to see the personal data your organization holds about them.
  - Under the GDPR you have a month to comply with such requests and may no longer charge a fee (unless request is manifestly unfounded or excessive, particularly if it is repetitive).

GDPR Core Concepts – Rights of Data Subjects

- **Right to rectification.**
  - Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
- **Right to restrict processing.**
  - Individuals have a right to 'block' or suppress processing of personal data.
- **Right to object.**
  - Individuals can object to certain data processing.

GDPR Core Concepts – Privacy by Design

- **Conduct data protection impact assessments (DPIAs).**
- **You must carry out a DPIA when:**
  - Using new technologies; and
  - The processing is likely to result in a high risk to the rights and freedoms of individuals.

GDPR Core Concepts – Data Protection Officer

- Under the GDPR, you **must** appoint a data protection officer (DPO) if you:
  - are a public authority (except for courts acting in their judicial capacity);
  - carry out large scale systematic monitoring of individuals (for example, online behavior tracking); or
  - carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

GDPR Core Concepts - Security

Security.

- Controllers and processors must implement technical and administrative measures to protect personal data.
- Appropriateness of measures based on:
  - State of the art and cost of implementation.
  - Nature, scope, context and purpose of processing.
  - Likelihood and severity of risks to the rights and freedoms of data subjects.

GDPR Core Concepts – Data Breach Notification

Data Breach Notification.

- A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed".
- Controllers must notify supervisory authorities within 72 hours of becoming aware of a data breach.
  - Notice content requirements.
  - Notice not required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of data subjects".

GDPR Core Concepts – Cross Border Data Transfer

Cross border data transfer

- Model Contract Clauses
  - Eliminated requirements for prior notice to DPA.
- Privacy Shield
- Countries
- Consent
- BCRs
- Codes of conduct/certifications
- Legitimate interests of data controller

GDPR – Do I care?

- **Does the GDPR apply to your organization?**
  - Do you process data from individuals resident in the EEA?

- **Penalties are significant (4% of annual worldwide turnover or 20 Million Euro, whichever is higher).**

- **Reputational risk.**

GDPR – Steps to take now

- **Raise awareness within your organization.**
- **Consider appointing a DPO (whether you need one or not).**
- **Identify the personal data you hold, why and on what basis you hold it, where it came from, how secure it is, and who it is shared with.**
- **Identify your lawful basis for processing.**
- **Review privacy policies.**

GDPR – Steps to take now

- **Review and update method for obtaining consent.**
- **Update data breach policy.**
- **Review and/or implement measures to legitimize cross border data transfer.**
- **Put together a DPIA template.**
- **Review process for subject access requests.**
- **Review and update contracts for GDPR compliance.**

Questions?

Shannon Yavorsky
Partner, Venable LLP
SKYavorsky@Venable.com

David Goodman
Global Non-Profit CIO
david@goodman.us.com