GDPR OVERVIEW: KEYS TO READINESS

THE EUROPEAN UNION (EU) IS IMPLEMENTING THE GENERAL DATA PROTECTION REGULATION (GDPR) THAT TAKES EFFECT MAY 2018.

2018

Satori CONSULTING

GDPR EXECUTIVE OVERVIEW

GENERAL DATA PROTECTION REGULATION

The objective of the GDPR is harmonization of EU regulations to enhance the rights of EU citizens to govern the *privacy* of their *personal information* and ensure organizations provide the right protections.

The GDPR applies to EU and non-EU organizations that:
(i) offer goods or services to EU residents;
(ii) monitor the behavior of EU residents

The GDPR effective date:
- May 25, 2018

Penalties:
- Up to 20,000,000 EUR or 4% worldwide revenue from the previous fiscal year (Article 83). Fines are determined by the Data Protection Authority (Supervisory Authority).

** The "Articles" referenced in this document refer to the articles included in the GDPR regulation. A link to the regulation text is included in the Appendix section of this document.*

GDPR EXECUTIVE OVERVIEW

GDPR CONCEPTS

Principles, privacy, and protection represent the core focus for GDPR readiness. Organizations must focus on adhering to principles, implementing processes to satisfy privacy rights of the individual, and securing data.

Principles

- Data processed lawfully, fairly, and transparently
- Only collect personal data needed
- Accuracy of personal data must be maintained
- Minimize the time data is kept in a form to identify data subjects
- Maintain the confidentiality and integrity of personal data

Privacy (rights of data subjects)

- Transparent information, communication and modalities for the exercise of the rights of the data subject
- Information to be provided where personal data are collected from the data subject
- Right of access by the data subject
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Right to data portability

Protection (controllers and processors)

- Data Protection Officer (DPO)
- Data protection by design
- Records of processing activities
- Security of processing
- Notification of a personal data breach to the supervisory authority
- Communication of a personal data breach to the data subject
- Data protection impact assessment
- Code of conduct

GDPR EXECUTIVE OVERVIEW

EXECUTION

GDPR requires the organization to address privacy and security of personal data. A proven approach to gaining clarity on GDPR relevance and understanding how to execute is described below. The Data Protection Officer (DPO) must lead the effort to achieve and maintain alignment.

Preparation

- Assign data privacy ownership
- Understand the regulation

Assessment

- Understand the risk of activities
- Perform Readiness Assessment

Implementation

- Inform the Organization
- Address consent
- Address rights of the individual
- Protect personal data

Maintenance

- Operationalize GDPR controls

GDPR EXECUTIVE OVERVIEW

KEY CONSIDERATIONS

GDPR readiness can be complex for some organizations. Leadership should begin to prepare the organization for the journey.

1. Key is establishing the DPO role (internal or external)
2. Gain clarity on the organization's responsibility
3. Complying with rights of the individual is not trivial – business processes, service desk, and technology impacts. Factor effort into 2018 budget – resource impact is key consideration (assuming good security practices).
4. Processor assessment is key – liability isn't shifted to the processor
5. Certification is not defined and is not required. DPA (supervisory authority) will assign certification bodies and certification guidelines. Move forward with readiness while tracking DPA guidance.

GDPR EXECUTIVE OVERVIEW

GDPR MISPERCEPTIONS

Understanding GDPR requirements can be complex. There are several common misperceptions that should be clarified.

1. A Data Protection Officer is required for all organizations
2. Each GDPR incident will carry a fine equivalent to the greater of 20 mil Euro or 4% annual worldwide revenue
3. Consent is always required for processing of personal data
4. Parental consent is always required when collecting personal information from a child
5. Individuals have the absolute right to be forgotten
6. Biometric data is sensitive data
7. Controllers do not require processing agreements with processors – GDPR takes care of this