The Security Leader's Guide to GDPR Compliance

Wednesday May 16, 2018
9:30 AM

Adam Stone
Principal Consultant and Chief Privacy Officer
Secure Digital Solutions, LLC

@secure360 facebook.com/secure360 www.Secure360.org

ENGAGE TO EMPOWER
Disclaimer

This presentation is for informational purposes only.

The content of this presentation does not constitute legal advice and should not be interpreted as such. Secure Digital Solutions, LLC is not a law firm. Consult a qualified attorney for questions pertaining to compliance with EU or US law.
Today’s Presenter

Adam Stone

MBA, FIP (Fellow in Information Privacy), CIPP, CIPM, CISSP-ISSMP, HCISPP, CHPS

Principal Consultant and Chief Privacy Officer, Secure Digital Solutions, LLC

18+ years experience in data security and privacy leadership and program development
Topics

Historical and Cultural Perspective

GDPR Basics

GDPR and Information Security

Data Flow Analyses

Data Protection Impact Assessments

Cross-Border Data Transfers and Privacy Shield

Security Leaders’ Next Steps

@secure360
Historical and Cultural Perspective

Drivers for Data Protection in the European Union
What Drives The Need for Enhanced Data Protection?
What Drives the EU’s Desire for Enhanced Data Protection?
### Charter of Fundamental Rights of The European Union

<table>
<thead>
<tr>
<th>Article 1</th>
<th>Article 6</th>
<th>Article 7</th>
<th>Article 8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human dignity</strong></td>
<td><strong>Right to liberty and security</strong></td>
<td><strong>Respect for private and family life</strong></td>
<td><strong>Protection of personal data</strong></td>
</tr>
</tbody>
</table>

- **Human dignity**
  - Human dignity is inviolable. It must be respected and protected.

- **Right to liberty and security**
  - Everyone has the right to liberty and security of person.

- **Respect for private and family life**
  - Everyone has the right to respect for his or her private and family life, home and communications.

- **Protection of personal data**
  - Everyone has the right to the protection of personal data concerning him or her.
  - Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
Data Privacy: Cultural and Institutional Differences

Trend towards collectivism
More trust in government
Less trust in corporations
Value privacy over convenience

Trend toward individualism
Less trust in government
More trust in corporations
Value convenience over privacy
Data Protection in the European Union – A (Very) Brief History*

January 28, 1981
Treaty regarding the protection of individuals’ personal data: Council of Europe Convention 108.

October 24, 1995

January 25, 2012
European Commission proposes a comprehensive reform of the Data Protection Directive to strengthen online privacy rights and boost Europe’s digital economy.

April 27, 2016

May 25, 2018
General Data Protection Regulation (GDPR) in force.

GDPR Basics
Understanding Relevant Portions of the Regulation
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure the integrity and confidentiality of the information to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information and otherwise to ensure compliance with this part by the officers and employees of such person.</td>
<td>Establish appropriate standards relating to administrative, technical, and physical safeguards to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.</td>
<td>This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data, protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, and ensures the free movement of personal data within the Union.</td>
</tr>
</tbody>
</table>

[Abridged] 42 U.S. Code § 1320d–2(d)  
[Abridged] 15 U.S. Code § 6801(b)  
[Abridged] Regulation (EU) 2016/679
Understanding GDPR at a Glance

Replaces ineffective legislation

Designed to harmonize compliance and enforcement across EU member states

Focused on balancing fundamental human rights and the EU Digital Single Market

Strengthens protections for individuals via rules on: consent, notice, data portability, and right-to-be-forgotten, among others
Focus of GDPR’s Data Protection Requirements

Sensitive Personal Data

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership,
- Genetic data
- Biometric data
- Health data
- Sex life or sexual orientation

Personal Data

- Demographic data
- Identification number
- Location data
- An online identifier

Data

All Data About a Given Data Subject
Key Business Activities In GDPR Scope

Data Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Cross-Border Processing

Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State, or

Data Transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation, subject to the provisions in GDPR.

Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
Who is In-Scope for GDPR?

Controller

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
# GDPR – Key Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lawfulness, fairness and transparency</strong></td>
<td>Processed lawfully, fairly and in a transparent manner</td>
</tr>
<tr>
<td><strong>Purpose limitation</strong></td>
<td>Collected for specified, explicit and legitimate purposes and not further processed</td>
</tr>
<tr>
<td><strong>Data minimization</strong></td>
<td>Limited to what is necessary</td>
</tr>
<tr>
<td><strong>Accuracy</strong></td>
<td>Accurate and, where necessary, kept up to date</td>
</tr>
<tr>
<td><strong>Storage limitation</strong></td>
<td>Stored for no longer than is necessary</td>
</tr>
<tr>
<td><strong>Integrity and confidentiality</strong></td>
<td>Protected against unauthorized or unlawful processing and against accidental loss, destruction or damage</td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td>Processing subject to legal obligations and accountabilities</td>
</tr>
</tbody>
</table>
“Data Processing”
Under GDPR

Processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

[Abridged] GDPR Art. 2(1)
“Data Processing” Under GDPR

Processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

[Abridged] GDPR Art. 2(1)
GDPR’s Coverage of Information Security Topics

- Data Privacy and Administration (98 out of 99 sections)
- Information Security (1 out of 99 sections)
Guiding Principles for Information Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

[Abridged] GDPR Art. 32(1)
## Applying the Guiding Principles

<table>
<thead>
<tr>
<th>Personal Data Processed</th>
<th>State of the Art</th>
<th>Costs of Implementation</th>
<th>Nature, Scope, Context and Purposes for Processing</th>
<th>Likelihood of a Negative Event</th>
<th>Severity of a Negative Event</th>
<th>Risk to Rights and Freedoms of Individuals in the EU</th>
<th>Risk Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human resources data</strong></td>
<td>Aging XYZ system deemed a “high” security risk due to several controls gaps. Compensating controls include high-grade firewalls and other industry-accepted network controls.</td>
<td>High cost of implementation (company plans to replace XYZ system with a newer, more robust solution).</td>
<td>Nature: Processing of human resources data. Scope: Applies to the processing of human resources data transferred from the company’s subsidiaries in the EU to the US. Context: Processing of human resources data required for EU-based employees. Purpose: Processing conducted for payroll, tax reporting, and benefits administration.</td>
<td>Likelihood is Medium-High (based on recent security risk assessment)</td>
<td>Severity is Medium (based on recent security risk assessment)</td>
<td>High risk to the rights and freedoms of EU-based employees</td>
<td>Mitigate within 6 months (by implementing the new HR system).</td>
</tr>
<tr>
<td>Marketing data</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Sales data</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Customer support data</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Accounts receivable and collections data</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
GDPR and Information Security

Article 32: *Security of Processing*

Pseudonymization and encryption of personal data

Ongoing confidentiality, integrity, availability and resilience of processing systems and services

Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Regularly testing, assessing and evaluating the effectiveness of technical and organizational measures
Data Flow Analyses

Understanding business processes
Data Flow Analyses

Critical activity

Scoping and segmenting suggested

Used to identify the movements and touch points of personal data

Results illustrate process flows and security controls for a given activity
Data Protection Impact Assessments (DPIA)
The Security Leader’s Guide
Data Protection Impact Assessment (DPIA)

No single “right” way to conduct DPIAs.

Article 29 Working Party provides updated guidance on DPIAs.

Rules for conducting DPIAs should be set in policy and/or standards.

At a minimum, DPIAs should be incorporated into your “project checklist” for each new/enhanced product.
Cross-Border Data Transfers

EU-U.S. and Swiss-U.S. Privacy Shield Framework
“The primary purpose of [GDPR’s cross-border data protection provisions] is to ensure that when the personal data of Europeans are transferred abroad, [GDPR’s protections travel] with the data.”

- European Commission*
Privacy Shield Principles

Notice
Choice
Accountability for Onward Transfer
Security
Data Integrity and Purpose Limitation
Access
Recourse, Enforcement and Liability
Continuing Your GDPR Journey…

Seek opportunities to add value to GDPR compliance.

Leverage existing security controls and processes.

Manage by business process, not technology.

Avoid signaling that the sky is falling.
Conduct a GDPR Readiness Assessment

- Evaluate Business Context
- Define Scope of GDPR Exposure
- Conduct GDPR Readiness Assessment
- Report Findings to Stakeholders
- Mitigate

Copyright © 2018 Secure Digital Solutions, LLC | All Rights Reserved.