Preparing for the GDPR

Orla O’Hannaighd - Womble Bond Dickinson
Agenda

- What is the GDPR?
- How Could it Apply to US companies?
- What are a Few Key Requirements?
- Share common challenges and steps companies are taking to implement the requirements
What is the EU General Data Protection Regulation (the “GDPR”)?

• EU privacy law
• Replaces current EU Data Protection Directive
• Effective May 25, 2018
• Applies to all EU/EEA Member States
  • What is the EEA?
  • What about the UK?
What does the GDPR Change?

• Risk of serious consequences for non-compliance
  • Fines of up to 4% of annual global turnover or €20 million
• Greater accountability
• Imposes direct obligations on those that “process” personal data
• For US companies → the extra-territorial scope is new
What is the GDPR?

**Key Definitions/Terminology**

- **Personal data** information related to a natural person that can be used to *directly or indirectly* identify the person
  - Name
  - Photo
  - Email address
  - Bank details
  - Posts on social media
  - Computer IP address

- **Special categories of personal data**: racial or ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic, biometric or health data, sex life or sexual orientation, criminal convictions/offenses
How Could the GDPR Apply to US Companies?

**Extraterritorial Reach – 3 Tests**

- **Establishment Test**
  - process data in the context of an EU establishment

- **Good/Services Test**
  - process data in relation to offering goods and services to data subjects in the EU

- **Monitoring Test**
  - process personal data in relation to monitoring the behavior of data subjects in the EU
A Few Key Requirements

Discussion of Requirements & Challenges

1. Guiding Principles
2. Legal Basis for Processing
3. Data Subject Rights
4. Accountability & Recordkeeping
5. Contract Amendments
6. Cross-Border Transfers
Key Requirements under the GDPR

1. Guiding Principles

**Data Protection Principles – Article 5**

<table>
<thead>
<tr>
<th>Personal data must be:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Processed lawfully, fairly and in a transparent manner</td>
</tr>
<tr>
<td>b. Collected for specific / explicit / legitimate purposes</td>
</tr>
<tr>
<td>c. Adequate, relevant and limited to what is necessary</td>
</tr>
<tr>
<td>d. Accurate (every reasonable step must be taken to rectify/erase inaccurate data without delay)</td>
</tr>
<tr>
<td>e. Kept in a form which permits identification for no longer than is necessary</td>
</tr>
<tr>
<td>f. Kept secure</td>
</tr>
</tbody>
</table>
Key Requirements Under the GDPR

2. **Lawful Basis for Processing**

To process personal data, must have a “lawful basis”:

- Consent of individual (this is “GDPR-level consent”); OR
- Processing is necessary for:
  - Performance of a contract
  - Compliance with a legal obligation
  - To protect vital interests
  - Performance of a public interest task
  - The purposes of legitimate interests
Key Requirements Under the GDPR

2. Lawful Basis for Processing (Cont’d)

- Clear communications to individuals
- Transparent privacy practices
- Result? Updated privacy policies/notices
- More disclosures about data practices
Key Requirements Under the GDPR

3. Data Subject Rights

- Individuals have lots of rights under the GDPR
- Individuals can request information and require action
- Company must respond to an individual’s request within 1 month (can extend the time if justified)
- At no cost (certain exceptions) to the individual
### Key Requirements Under the GDPR

#### 3. Data Subject Rights

<table>
<thead>
<tr>
<th>Art</th>
<th>Right of Data Subject</th>
</tr>
</thead>
</table>
| 15  | Right of access to personal data  
*Can obtain a copy of all personal data held by company* |
| 16  | Right of rectification  
*Can have personal data corrected* |
| 17  | Right to erasure / to be forgotten  
*Can have personal data deleted in certain instances (e.g., if no longer necessary for the purposes for which it was collected, consent is withdrawn, etc.)* |
| 18  | Right to restrict processing  
*In certain situations can ask to suspend use of personal data (e.g., if data is inaccurate and needs to be verified)* |
| 20  | Right to data portability  
*Can obtain data in a structured, commonly used and machine-readable format. Applies when use is based on consent or performance of a contract and when use is by automated means* |
### Key Requirements Under the GDPR

#### 3. Data Subject Rights Continued

<table>
<thead>
<tr>
<th>Art</th>
<th>Right</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Right to object – including right to object to direct marketing and profiling related to direct marketing</td>
</tr>
<tr>
<td>77</td>
<td>Right to complain to the regulator</td>
</tr>
<tr>
<td>79</td>
<td>Right to judicial remedy against a controller / processor</td>
</tr>
<tr>
<td>80</td>
<td>Right to representation (by consumer bodies / watchdogs)</td>
</tr>
<tr>
<td>82</td>
<td>Right to compensation from controller / processor</td>
</tr>
</tbody>
</table>
Key Requirements Under the GDPR

4. Accountability Principle

• Must be responsible for and able to demonstrate compliance with the GDPR
• Requires companies to closely identify and document all data flows and usage
• Must respond to and notify when data breach
• May be required to appoint a Data Protection Officer and/or local EU representative
Key Requirements Under the GDPR

5. Contract Remediation

• “Controller” **must** have a contract in place with any “processor” (e.g., vendor)
• Contract must include very specific provisions
• **Result**  ➔ Controllers and processors have to amend existing contracts and revise templates going forward
Key Requirements Under the GDPR

6. Cross Border Transfers

• If personal data is transferred outside of the EU to another country, then must have a mechanism in place
• Multiple GDPR-approved mechanisms
• Most common:
  • Model clauses (approved by the EU Commission)
  • Join the EU-US Privacy Shield