GDPR: Are You Ready?
Mapping the Road to GDPR Compliance
March 2018
Agenda

• GDPR Overview
• Should you appoint a DPO?
• Accountability checklist/documentation required
• When is consent appropriate and how do you manage it?
• What can we expect with Data Subject Requests?
• Top 5 Steps to take now to reduce risk
• Technology tools
GDPR Overview

• What Is the General Data Protection Regulation (GDPR)?
• Which Businesses Must Comply?
• Why Should Companies Care?
• Key changes
• Mapping a Practical Course to GDPR Compliance
A New Level of Data Protection

• The GDPR is the EU’s new data protection law
  • Imposes a uniform data protection law on all EU Member States
  • Provides for the creation of a European Data Protection Board (EDPB) and role of “lead SA” where organization has its “main establishment”
• Enforceable on 25 May 2018
Scope of the GDPR
(Articles 2, 3)

• **Broadens** Territorial Scope
  
  • GDPR applies directly to controllers and processors established in the EU (place of processing indifferent)
  
  • GDPR applies to non-EU companies if they **target the EU market** by
    
    • offering their goods or services to individuals located in the EU (whether or not payment is required), or
    
    • monitoring their behavior

**Impact:** Applies to *any* company that markets goods or services to individuals located in the EU regardless of whether the company is located or uses equipment in the EU.
Applies to Data Processors
(Articles 3(1), 30-33, 36-37, 44)

What Are “Data Processors”?  
- Organizations engaged by a controller to process personal data on its behalf (e.g., as an agent or service provider – includes, e.g., payroll service providers)

  - **What Is Processing?**  
    Any actions performed on personal data whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Processor Obligations
- Maintain adequate **documentation** regarding all categories of personal data processing activities carried out on behalf of a controller
- Implement appropriate **security** measures
- Comply with rules on **international data transfers**
- Appoint a data protection officer (**DPO**) in some cases
Why Should Companies Care

• **Operations**: Will require significant changes to how non-EU companies manage personal data collected from individuals in the EU

• **Penalties**: Increased fines could adversely impact your operations, and possibly put some companies out of business

• **Oversight**: Supervisory Authorities have new and expanded enforcement powers

• **Remedies**: Individuals now have judicial remedies against controllers and processors
Expanded Enforcement Powers
(Article 58)

**INVESTIGATORY**

- order production of information
- carry out investigations/audits
- obtain access to all personal data held by controller/processor and all relevant information if necessary to perform regulatory functions
- obtain access to premises, processing equipment, etc.

**CORRECTIVE**

- order controllers or processors to comply with data subjects’ rights and to bring processing operations into compliance
- order erasure of personal data
- impose temporary or definitive limitations on operations, including a ban on processing
- order suspension of data flows to recipients in third countries
Judicial Remedies
(Articles 78-82)

• Data subjects have right to effective judicial remedy against SA, controller and processor

• Data subjects have right to compensation from controller and/or processor for material or "immaterial" (i.e., non-pecuniary) damages suffered

• Possibility of "class actions" by not-for-profit organizations on behalf of data subjects
  • Member States can allow such organizations to make claims even without a data subject’s mandate
Key Changes

• Broader Definition of Personal Data
• Increased Sanctions and Penalties
• Data Processors Regulated
• Data Governance and Accountability
• Higher Bar to Document Consent
  •  (Customers and Employees)
• Increased Individual Rights
Mapping a Practical Course to Compliance

- Governance
- Documentation
- International Transfers
- Customer Data
- Human Resource Data
- IT/Security
Main Projects For Most Organizations

<table>
<thead>
<tr>
<th>Data Map</th>
<th>Vendor Management</th>
<th>Retention</th>
<th>HR Consent &amp; Notice</th>
<th>Lead Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent &amp; Notice</td>
<td>Collection</td>
<td>Privacy by Design</td>
<td>HR Individual Rights</td>
<td>Data Governance</td>
</tr>
<tr>
<td>DSAR Systems</td>
<td>Individual Rights</td>
<td>Training</td>
<td>HR Security</td>
<td>Incident Response</td>
</tr>
<tr>
<td>Profiling</td>
<td>Security Measures</td>
<td>DPIA</td>
<td>DPO</td>
<td>Verification</td>
</tr>
<tr>
<td>Privacy Policies</td>
<td>Works Council</td>
<td>Centralized Repository</td>
<td>Cyber Insurance</td>
<td>Code of Conduct</td>
</tr>
</tbody>
</table>
To Appoint or Not to Appoint

Do You Need to Appoint a DPO?
If Not, Should You?
Mandatory DPO under the GDPR
(Article 37)

• DPO requirement applies to both controllers and processors
• No exception for small or medium-sized companies, but risk-based approach
• The GDPR requires the appointment of a DPO in three cases:
  • Public authorities or bodies (except courts)
  • Private companies where the “core activities” consist of
    • processing operations which require “regular and systematic monitoring” of data subjects “on a large scale”
    • “large scale” processing of sensitive data or data relating to criminal convictions and offences
    • if obligated by local laws
Data Protection Officers (DPO) (Articles 37-39)

• DPO can be a “qualified” staff member or an external provider (services contract)

• Reports to highest level of management

• Must have professional qualities and expert knowledge of EU DP law
Consequences of DPO

• **What are the risks with appointing a DPO?**
  • If you voluntarily appoint a DPO, must comply as if it is a mandatory appointment
  • Difficult to remove, cannot terminate for approach to GDPR compliance
  • Must involve appropriately in business activities
  • Must provide appropriate support
  • Failure to appoint or provide support, could subject company to fines

• **What are the benefits of appointing a DPO?**
  • In-house data rights expert/first point of contact with data subjects and regulators
  • Someone at a high level who understands the technicalities of the regulation
  • Sends the message to customers that you take compliance seriously
  • Can help explore and assess new business opportunities that utilize data assets
Accountability Checklist/Documentation

- Data protection impact assessments
- Consent forms
  - Request as little data as possible
  - Make the terms and conditions clear
  - Make it easy to withdraw consent
- A description of the data protection officer role
- A data breach notification procedure
- Subject access request forms and procedures
  - Under the GDPR, all organizations need to give individuals the right to obtain:
    - Confirmation that their data is being processed;
    - Access to their personal data; and
    - Other supplementary information (mostly the information provided in privacy notices)
Significant lift for most companies – data processing records

- **Data controllers** must keep a record of their processing activities including the purposes of the processing, description of the categories of data subjects and of personal data, categories of recipients, transfers of personal data to third countries, retention periods, and description of security measures in place to protect personal data.

- **Data processors** must maintain a record about processing activities carried out on behalf of a controller, including the categories of processing, cross border data transfers and security measures that have been implemented.
Consent Requirements
(Articles 6 -9)

- **EU Directive**: express or implied consent permitted
- **GDPR**: requires consent be freely given, specific, informed and unambiguous

> “any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed”

- Must keep records of consents
- Cannot bundle consents

**Impact**: Companies should analyze their current consent process and revise so they are specific, clear, prominent, opt-in, documented and easily withdrawn.
Consent

• When is it appropriate to use consent as the legal basis for processing?
  • When it can be freely given
  • When you can provide clear notice
  • If it can be withdrawn at any point (hard to do with employment data or data necessary to fulfill a business agreement)

• How should you obtain consent?
  • EU data protection law does not specify the method by which consent should be obtained.

• How can you manage consent and the ability of data subjects to withdraw it at anytime?
  • May require businesses to create new systems and procedures to satisfy this requirement.
Data Subject Access Requests (DSARs)

• What can we expect?
• How can we manage?
  • Timeframe for complying with a DSAR = one month (can extend this deadline by up to two months if the requests are complex or numerous)
  • If an individual makes a DSAR by electronic means, the employer must provide its response in electronic form too (unless otherwise requested by the individual)
  • An employer can charge a reasonable fee (taking into account its administrative costs) and can refuse to respond where a request is manifestly unfounded or excessive
Expanded Individual Rights
(Articles 15-17, 19-22 – Access, Deletion, Correction, Portability)

• **Data Subject have the right to have all personal data deleted** without undue delay when:
  - Consent withdrawn
  - Retention not required
  - Data no longer needed
  - Court or SA orders data must be erased

• Data controller must also inform downstream third parties of the data request - “disproportionate effort” exception

**Impact:** Companies should devote time and resources to developing procedures to manage personal data in a way to enable efficient erasure.
Expanded Individual Rights

- **Right to data portability**
  - Individuals have the right of access to their personal data in a commonly used electronic form
  - Limited to data provided knowingly and actively by the individual to the data controller
  - Only applicable for data obtained on the basis of consent or contract (not legitimate interests)
  - Does not apply to profiling or inferred or derived data created by the controller on the basis of data provided by the individual

**Impact**: Companies should have procedures in place to manage personal data in a way to enable efficient portability.
Top 5 Steps to Take Now to Reduce Risk

• Prepare GDPR-compliant notices for employees, customers, website visitors
• Update your employee agreements and customer and vendor contracts
• Implement an appropriate data transfer mechanism for cross-border transfers
• Establish mechanisms to receive and respond promptly to data subject requests (access, erasure, portability, etc.)
• Create a GDPR-compliant data breach response checklist to be integrated into a compliant Incident Response Plan
In conclusion…

- This is a **process** so stay calm, get organized and get started
- Assess the true **impact** on your business operations
- Prioritize **accountability**/record keeping
- **Think strategically** about your data flows