Preparing for the EU General Data Protection Regulation

May 25, 2018

Effective date of the EU General Data Protection Regulation

- Significant new regulation affecting the use and transfer of “personal data” in the European Union
- Backed by significant new penalties for non-compliance including the greater of €20 million or “4% of annual worldwide turnover”

Develop a Timeline

Timeline and Project Plan

1. February 2018
   - Decide Whether to Appoint a Data Protection Officer (DPO), even in the absence of a legal requirement. French Data Protection Authority (Commission Nationale de l’Informatique et des Libertés [CNIL]) in March 2017, regarding best practices to demonstrate GDPR compliance by May 2018. CNIL in the past data protection authority in France issued guidance for GDPR compliance, now removed. More about the FSB’s guidance on Alston & Bird’s Privacy Blog in post titled: French CNIL Releases GDPR Compliance Toolkit. The tasks and proposed dates are set forth below. For those who would like more detail, please refer to the budget draft uploaded on the Alston & Bird site.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Activity Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase I</td>
<td>Appoint Data Protection Officer</td>
<td>February 2018</td>
</tr>
<tr>
<td>1.</td>
<td>Decide Whether to Appoint a Data Protection Officer (DPO), even in the absence of a legal requirement.</td>
<td>French Data Protection Authority (CNIL) in March 2017, regarding best practices to demonstrate GDPR compliance by May 2018. CNIL in the past data protection authority in France issued guidance for GDPR compliance, now removed. More about the FSB’s guidance on Alston &amp; Bird’s Privacy Blog in post titled: French CNIL Releases GDPR Compliance Toolkit. The tasks and proposed dates are set forth below. For those who would like more detail, please refer to the budget draft uploaded on the Alston &amp; Bird site.</td>
</tr>
</tbody>
</table>
Applies Broadly to “Processing” of “Personal Data” of EU Residents

- "Personal data" means any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- "Processing" means any operation or set of operations performed on personal data or on sets of 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.

Applies to businesses that offer goods or services to EU residents or monitor the behavior of EU residents.

EU Regulators Eager to Start Enforcing the GDPR

Selected Key Requirements

- Update privacy notices to identify (a) legal bases for processing; (b) legitimate interests pursued; (c) retention periods; and (d) transfer recipients (Art. 13-14)
- Maintain detailed written records of all processing activity, and the legal basis for that processing (Article 30)
- Privacy by Design and Privacy by Default
- PIUs and DPOs
- Expanded Individual Rights
“Privacy by Design” and “Privacy by Default” Required

- Limit retention
- Minimize use of personal information

PIAs

- Data Protection Impact Assessments are required if
  - (i) “high risk” to rights and freedoms,
  - (ii) profiling/automated decision-making that legally or significantly affects individuals, or
  - (iii) “large scale” sensitive data processing.

Data Protection Officer must be designated if “the controller’s or processor’s ‘core activities’ require ‘regular and systematic monitoring of data subjects on a large scale’ or consist of ‘processing on a large scale of special categories of data.’”

- “core activities” and “large scale” not defined
- “Special categories of data” –
  - Race
  - Political
  - Religion or “philosophical beliefs”
  - Trade union membership
  - Genetic, biometric, health data or data regarding sex life or sexual orientation

- Think: HR? Marketing, mass communications, or “Big Data” analytics of individuals?
- Other activities?
Data Protection Officers:
• required to have “expert knowledge of data protection law and practices;”
• must report to the “highest management level” of the organization; and
• can’t be fired or “receive any instructions” regarding the exercise of tasks.

Also required for processors – significant for companies who don’t have EU locations but who have EU clients or customers

Expanded Individual Rights
• Data Access
  • Right to know purpose of processing, categories of data concerned, the “existence of automated decision-making,” and “meaningful information about the logic involved.”
• Data Portability
  • Right to usable (machine-readable) copy of information concerning the data subject
• Right to Object
• Right to Rectification
• Right to Erasure

Other Requirements
• Must notify supervisory authority within **72 hours** of “becoming aware” of a data breach
• Recordkeeping (individual rights requests, consents, refusal of access, refusal to stop processing, record processing activities)
• Subcontracting (mandatory outsourcing / subcontracting requirements, including contractual flow-downs)
• New children’s privacy provisions
Penalties

- For controllers and processors
- Greater of €10M or “up to 2% of the total worldwide annual turnover of the preceding financial year” for (e.g.):
  - Failure to obtain proper parental consent for processing children’s data
  - Failure to adhere to principles of data protection by design and by default
  - Failure of your DPO to perform tasks properly

Greater of €20M or “up to 4% of the total worldwide annual turnover of the preceding financial year” for:

- Failure to adhere to “principles of processing” to collect data for “specified, explicit and legitimate purposes” and not process otherwise;
- Failure to adhere to data minimization or data retention requirements;
- Failure to maintain “appropriate” security;
- Failure to process data based on one of 6 specific identified bases for process; or
- Failure to give effect to the data subjects’ expanded rights

Other Enforcement/Penalties

- Also empowers individual data subjects by authorizing actions against DPAs, against controllers or processors, by authorizing non-profits to represent individuals, by authorizing compensation for data subject damaged by violation
- And also..... member states may impose “other penalties”
What We’re Doing to Help

• Roadmap to GDPR Series
• Blog Posts
• Major Engagements
  • World’s largest logistics company, largest fast-casual dining company, major global data security and hospitality firms, etc.
  • Data mapping, review of organizational controls, vendor contracting, updating notices, gap analysis, review of key systems (CRM, HR, systems where data subject may exercise rights)

Recognizing and Responding to GDPR Issues

• How to identify whether your client has an issue?
  • First step is easy: customers or employees in the E.U? any processing of EU “personal data”?

  • Next Steps:
    • These can be significant projects for large organizations
    • Should be working on this NOW / yesterday.

Global Compliance Checklist

- Identify the Countries that are critical for your business
- Understand whether you have cloud vendors or other vendors that might trigger compliance obligations
- Conduct privacy/security due diligence
- Be Aware of key developments in the EU, China, and US
- Train and Engage Your Employees
Cross-Border Transfer Laws

European Union
Russia
Switzerland
China
South Korea

Synthesizing Analysis on Data Transfers in APEC (Examples)

Global Laws – Requiring Vendor Management

- Article 44 - processor
- Privacy Shield
- Contractual requirements for vendors to comply with (1) Security and (2) Accountability for Onward Transfer Principle
- Chinese Network Security Law (effective 6/1/17)