PRIVACY ASSOCIATES INTERNATIONAL LLC

Top Things You Should Do (Or Should Have Already Done) In Preparing For EU GDPR Compliance

SMB IT Law Section Privacy Law Committee Meeting

Robert L. Rothman
Keith Cheresko

June 15, 2017

Purpose

- Review selected preparatory matters for GDPR compliance
- Concentrate on long lead-time items
- Discuss how these matters are being addressed by us and our clients

Determine Whether Your Organization is Subject to the GDPR

Determine Whether Your Organization is Subject to the GDPR

- Organizations with establishments in the EU (e.g. subsidiaries) regardless of where processing occurs
- Organizations outside the EU
  - Offering goods and services to persons within the EU
  - Monitoring behavior of data subjects within the EU (includes tracking, creating profiles etc.)

Dealing with the Expanded Individual Rights Under the GDPR

Consent

Consent

- Ensure your collection and processing of consent meets the revised conditions under GDPR
- Additional conditions under GDPR
  - Includes an effective prohibition on “bundling”
  - Supply of service cannot be made contingent on consent to processing that is not necessary for the service requested
  - Must be separable from other written agreements, clearly presented and easily revoked as given
- Specific rules for children

Right To Erasure

Right To Erasure (To Be Forgotten)

Establish processes and procedures to address requests to erase information received from data subjects

- If you made the personal data public and receive an RTBF request, you have to 'take reasonable measures' to inform 3rd parties who are processing the data that an RTBF request has been made
- Not unlimited – narrow exemptions for, e.g., freedom of expression, research purposes, EU legal obligation & claims
- Also establish processes and procedures to address requests to restrict processing received from data subjects

PAI

Right To Data Portability

Right To Data Portability

Review and establish as necessary processes to transfer personal data upon request of a data subject

- Facilitates individual's ability to move data to another party, by requiring the data controller to:
  - Provide a copy of personal data in "commonly used" electronic and structured format
  - Upon request provide directly to other party
- Applies to personal data about the individual
  - Provided by the individual
  - When obtained via consent or contract
- Data Portability should not adversely affect other individuals' rights and freedoms

PAI

Right To Data Portability

- One month to comply, which can be extended to max. 3 months for complex cases
- Method: Data should be made available preferably by a direct download (extraction) opportunity
- Other means are secured messaging, an SFTP server, a secured WebAPI, or WebPortal
- Provide using commonly used open formats (e.g. XML, JSON, CSV) along with useful metadata at the best possible level of granularity

PAI

Data Subject Notices

Data Subject Notices

Assess and revise consumer facing notices to provide:

- Contact details
- Purpose for processing
- Recipients of information
- Details of transfers outside to EU
- Retention period for the data
- Right to access and portability
- Right to rectify, erase, and restrict processing
- Ability to complain to supervisor authority
- Use of automated decision-making

All in a concise, transparent, intelligible and easily accessible manner

PAI

Right To Data Portability

Right To Data Portability

- One month to comply, which can be extended to max. 3 months for complex cases
- Method: Data should be made available preferably by a direct download (extraction) opportunity
- Other means are secured messaging, an SFTP server, a secured WebAPI, or WebPortal
- Provide using commonly used open formats (e.g. XML, JSON, CSV) along with useful metadata at the best possible level of granularity

PAI

Suppliers

Supplier Contracts

Review your contracts with suppliers because revisions are likely necessary

- Must be in writing (including in electronic form)
- Must contain specific descriptions (subject matter and duration, nature and purpose of processing, type of personal data and categories data subjects, obligations and rights of the controller)
- Must contain specific obligations for the service provider
- Commission may adopt standard contractual data processor clauses

Supplier Contracts

- More obligations to address in third-party contracts with suppliers:
  - Assist controller in responding to individuals' requests (Data portability may require attention)
  - Assist the controller in ensuring compliance
  - Make available to the controller and the DPA all information necessary to verify compliance with the foregoing obligations
- In fact, accountability requirement on suppliers

PAI

Direct Obligations for Suppliers

Direct Obligations for Suppliers

If you are a supplier subject to the GDPR, review your operations to ensure that you:

- Designate an EU representative if not established in the EU
- Process on instructions of controller only
- Ensure that sub-processors are engaged only with the controller's prior authorization
- Maintain required documentation and provide to DPA at request
- Cooperate with DPAs
- Implement security measures and ensure that controller is notified of a security breach

Direct Obligations for Suppliers

If you are a supplier subject to the GDPR, review your operations to ensure that you:

- Designate a DPO (where applicable)
- Comply with cross-border transfer requirements
- only act on documented instructions from the controller, including with regard to cross-border transfers to countries outside the EU
- Some cases: inform the controller if an instruction of the controller breaches the GDPR
- at choice of controller, delete or return all data to the controller after the end of the processing, and delete all copies unless EU law requires storage

PAI

Supplier Contracts: Subcontracting

- Allow supplier to use subcontractors only with the prior permission of the company (controller)
  - If general authorization, still inform controller about intended changes and give an opportunity to object
- Suppliers must impose same data protection obligations on the subcontractor
- GDPR provides that the supplier shall remain fully liable to the company for the performance of the subcontractor

PAI

Compliance Requirements

Record Keeping

Record Keeping

- Replaces current requirements to register with DPAs
- Records must be made available to DPA on request
- Maximum fine for not keeping record or not sharing with DPA: 2% global turnover / EUR 10 mil.

Record Keeping

Make necessary modifications to record keeping to meet GDPR requirements

- Requirement to maintain records of all processing activities (art. 30)
  - Description of categories of data subjects and categories of personal data
  - Purposes of processing
  - Categories of recipients
  - Transfers to third countries (including identification of the country and adequacy mechanism)
  - Where possible, envisaged time limit for erasure
  - Where possible, general description of security measures
  - Name and contact details of (joint) controller and DPO
- Similar recordkeeping obligations for processors

PAI

Record Keeping

- Record legal basis for each processing purpose is not required, however most companies are including legal basis in registry
  - Notice content requirements under GDPR include informing individuals about legal basis for processing their data

Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessment

Institute where necessary a Data Protection Impact Assessment process separate from the Record Keeping

- Requirement to carry out DPIA prior to undertaking a high-risk processing (art. 35)
- Requirement to consult DPA when DPIA shows there is residual high risk even after mitigation measures are taken
- Especially new technologies and taking into account the nature, scope, context, and purposes of the processing

PAI

What Is “High-Risk” Processing?

- Any profiling on which decisions are based that produce a legal effect or similarly significantly affect individual (in fact art. 20)
- Large scale processing of sensitive data, or of data relating to criminal convictions and offenses (or related security measures)
- Systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV)

Conclusion

- This session has only touched some of the topics and concepts involved in GDPR readiness
- GDPR compliance is not easy and the failure to comply is designed to be very costly
- Done correctly it takes considerable resources (e.g. people, time and budget) to fully understand and revise elements of your operation that may be impacted
- It is not a once and done exercise – the member state laws are being amended and guidance for many of the undefined elements have yet to be issued
- Don’t wait to get started – May 2018 is fast approaching especially for revisions to contracts, notices, information systems and record keeping