PAI PRIVACY ASSOCIATES INTERNATIONAL LLC

The GDPR is Here: Now What?

10th Annual Information Technology Law Seminar
September 7, 2017

Keith A. Cheresko & Robert L. Rothman, Principals,
Privacy Associates International LLC

Purpose

- Give you a general understanding of the EU's General Data Protection Regulation (GDPR) and its importance to you and your clients
- Focus on jurisdictional and practical preparation issues
- Privacy Shield

What is the GDPR?

- A Regulation designed to increase the data protection afforded data subjects in the EU.
- As a Regulation it is a binding law directly applicable in all Member States – like a US federal law
- Several years in the making adopted April 27, 2016 with an effective date of May 25, 2018

Okay, but why should **American** companies be concerned about this European legislation?

Determine Applicability to US Entity

- GDPR applies to the processing of the personal data of EU persons by a controller or processor **in the US** where the enterprise:
  - Has an "establishment" (e.g. subsidiary) in the EU
  - Offers goods or services to EU persons
  - Monitors the behavior of the EU persons
  - Is subject to an EU state law by virtue of public international law

Determine Applicability to US Entity

- Maintaining a website in the US offering goods or services that can be accessed by European persons does not alone confer jurisdiction
- Maintaining a website in the US offering goods or services may confer jurisdiction if:
  - The website is available in the language of an EU member state
  - EU currencies are accepted
  - EU customers or users are mentioned, as in testimonials

PAI

Determine Applicability to US Entity

- Monitoring the behavior of EU persons may involve:
  - Tracking
  - Profiling
  - Behavioral advertising generally
- Not necessary to be dealing with the actual name of the EU person: IP address is sufficient

PAI

Potential Monster Fines and Private Actions Transform Privacy Risk Profile

- Under GDPR, private actions, including group actions allowed and fines go up to 4% of global turnover (revenue based on prior year) or Euro 20 Million, whichever is **greater**
  - Bet the business levels
  - Tantalizing new revenue source for EU countries
- Fines imposed based on group activity, not an individual group company

Some Examples

- Based on 2015 financial results, fines could be:
  - $5,982,320,000 for Ford
  - $6,094,400,000 for GM
  - €4,423,800,000 for FCA
  - $4,696,000,000 for GE
  - $1,408,000,000 for Deloitte
  - $1,416,000,000 for PwC
- Privacy carries new levels of organizational risk

PAI

What Companies and Law Firms Should Be Doing **Now** to Prepare for the GDPR

- Many enterprises have been working at GDPR compliance for many months
- If you haven't started don't wait any longer - get started -- with a plan
- Tasks are complex and time consuming requiring people, IT, and budget resources
- Compliance for covered entities is mandatory May 25, 2018

PAI

Starting Point: Awareness

- Ensure decision makers and key personnel are aware of the changes coming under GDPR
- Evaluate the likely impact and identify areas of concern where gaps are present
- Designate and assign responsibilities to personnel for planning and implementing necessary changes
- Raise in-house awareness through training
- Modify privacy audit and review processes with the GDPR in mind

Data Mapping

- Conduct data mapping and document EU personal data handling
  - What you have
  - Where it came from
  - With whom you share it
  - Legal bases used today for processing, including transferring, European PII
  - Comply with the accountability principle

Privacy Notices to EU Persons

- Your privacy statements will almost certainly have to be redrafted, as will the processes for delivering them
- Examples of disclosures that MUST be included:
  - The identity and contact details of your Data Protection Officer (if any)
  - If the processing is based on the controller's legitimate interests, an explanation of those interests
  - The data retention period
  - A brief explanation of the rights to erasure and to object to processing
  - the right to complain to the Supervisory Authority
  - Information on cross-border data transfers.
  - Where the personal data are not obtained directly from the data subject, the source of the data
- Look for standardized, machine-readable icons to supplement these privacy notices in the future

PAI

Consents

- Understand where you are using consent as a basis for processing or transferring the data of an EU person
- If you have made the provision of a good or service conditional on consent where the consent is not inherently necessary, reorganize the business process because it no longer is valid for EU persons
- Make certain you can defend the consents as having been freely given, not the subject of unequal bargaining power (e.g. employment situation)
- Make sure that the data subject has to perform some affirmative action to agree and that you retain documentation
- If part of another document, see that the consent language is clearly distinguishable and in plain language
- Create processes that make it as easy to withdraw consent as it was to get it in the first place

Restrict Processing

- You need create a hold process so upon request during a dispute an individual's data will be held and not used by you
- You may further process
  - If the data subject consents
  - If it is necessary for establishment of legal claims
  - For protection of the rights of another individual
  - For reasons of public interest (e.g. EU or Member State)
- Where data is processed automatically a technical solution is necessary to flag or segregate the data until the restriction is resolved.
- Policies and practices sufficient to allow the storage, blocking, retrieval and notice to the individual before lifting the restriction

PAI

Portability

- You must create processes and systems that will allow you to comply with the right of a data subject to have his data in your possession provided by him transferred to the data subject or a third party where
  - The Personal Data was processed by automated means
  - Basis of processing is consent
  - Data being processed to fulfill contract or steps preparatory to a contract
- This can require you to furnish customer information to a competitor

Profiling

- You must have processes to effectuate individuals' rights not to be subject to any decisions made using automated processing of personal data (profiling)
- You may use profiling to evaluate individuals if:
  - necessary to enter into, or to perform, a contract between a data subject and you
  - authorized by EU or Member State law, or
  - based on the individual's explicit consent
- In cases of contract performance and consent, you must implement suitable measures to safeguard the data subject. At a minimum,
  - A right to obtain human intervention for the data subject to be able to express his or her point of view
  - The ability to contest the automated processed decision.

PAI

Erasure (Right to be Forgotten)

- You must put in place processes that allow for the erasure (not suppression) of information upon request of the data subject when, e.g. :
  - The data is no longer needed for its original purpose
  - The processing is based on consent, and the data subject withdraws that consent
  - The data subject exercises the right to object
  - The processing is unlawful
- If you have already made the information public the processes must include the taking of “reasonable steps” to tell others who are processing the information of the request (subject to certain US First Amendment-type exceptions)

PAI

Access

- Make revisions to your processes to make certain you can provide data subjects, upon request, GDPR-required information
- You also have to be prepared to:
  - Disclose whether and where data subject information is being held or processed
  - Give access to and copies of the data
  - Provide additional information such as
    - The purpose of your having the information
    - The recipients or types of recipients of the information
    - Information regarding the retention period
    - The source of the information
    - The safeguards in place if an international transfer is involved

Data Breaches

- Your data incident response plan will undoubtedly have to be modified in order to comply with the new GDPR rules
- In particular, your plan must provide for notifying the appropriate European Supervisory Authority of an incident “without undue delay” and “where feasible not later than 72 hours after having become aware of it”
- If the 72 hour limit is not met, you will have to justify why
- You will need to keep GDPR-specified records of the incident and your response for review by the authorities
- Notice to individuals without undue delay where there is a high risk to rights and freedoms

Record-Keeping

- If you are a US organization subject to the GDPR, new internal processes may well have to be created to be able to keep track of all EU personal data processing and be able to make such information available to European Supervisory Authorities upon request
- The records must include:
  - Details of the controller and the Data Protection Officer, if any
  - The purposes of the processing activities
  - The categories of personal data and data subjects
  - Details of any recipients of the data
  - Applicable retention periods
  - Security measures
- Most of these rules equally applicable to controllers and processors

PAI

Data Protection Officer

- You will be required to appoint a Data Protection Officer when you
  - are processing sensitive data on a large scale
  - are conducting regular and systematic monitoring of individuals
- Good practice where not mandatory
- The DPO must operate independently and not take instructions from the business as to the exercise of his or her functions
- The DPO must report to the management of the business
- Align function's responsibilities with GDPR requirements

Data Protection Impact Assessments

- You must use a Data Protection Impact Assessment (DPIA) to identify and minimize risks of non-compliance when data processing is likely to have high impact on privacy
- Establish policies and procedures to standardize and document the DPIA process and results obtained
- When a DPIA shows a high impact is likely (and mitigating factors do not work) you must have a consultation with the DPA and address privacy protections before proceeding

Data Protection by Design and Default

- Implement technical and organizational measures showing data protection is a consideration for all your processing activities
  - Adopt staff policies mandating use
  - Integrate into IT development practices and document use
  - Audit for use

Children

- You need to put COPPA-like processes in place for European children
- Processing of personal data of a child below the age of 16 years requires the consent by the parent or other holder of parental responsibility
- Member States can lower the age threshold (but not below 13 years)
- You must be able to document that you make reasonable efforts to verify the parental consent has been properly given

Privacy Shield

- The Privacy Shield is an administrative agreement between the US through the Department of Commerce and the EU under which companies that certify compliance with the Privacy Shield Principles are deemed adequate to process EU data
- The Edward Snowden revelations of the extent of US government surveillance domestically and overseas raised suspicion and backlash around the world – seemingly undiminished by terrorist events in Europe
- Partially as a result, the European Court of Justice invalidated the EU-US Safe Harbor arrangement allowing the transfer of EU personal data to the US
  - Basis was the EU Charter of Fundamental Rights and the inadequate assurances US companies could protect the data from the US government
  - This makes other cross-border transfer mechanisms legally uncertain

PAI

Privacy Shield

- The EU Commission and the Department of Commerce reached agreement on a EU-US "Privacy Shield" with added obligations on the US side to act as a Safe Harbor replacement
  - Privacy Shield in place since February 2016
  - Being challenged in EU on same basis as Safe Harbor was challenged
  - 2,472 US companies have self certified
  - Review process

Contact Information

Keith A. Cheresko

Privacy Associates International LLC

kcheresko@privassoc.com

www.privassoc.com

(248) 535-2819

Robert L. Rothman

Privacy Associates International LLC

rrothman@privassoc.com

www.privassoc.com

(248) 880-3942