PRIVACY ASSOCIATES INTERNATIONAL LLC

2016 European Privacy Update

ISACA

April 20, 2016

Keith A. Cheresko, Principal **Robert L. Rothman, Principal**
Privacy Associates International LLC

Purpose of Presentation

- Brief discussion of the massive changes in the privacy world in the last few months
- High level introduction of the General Data Protection Regulation – the “GDPR”
- Suggestions as to what companies should be doing now

The Legal & Political Privacy Environment

Last Time

When we last spoke in 2014:

- We presented information about the proposed EU data protection regulation in the works to replace the Privacy Directive
- Safe Harbor was an effective means to transfer personally Identifiable Information (PII) from the EU to the US
- No one knew the extent of US government surveillance of Non-US citizens

Now

- The Edward Snowden revelations of the extent of US government surveillance domestically and overseas raised suspicion and backlash around the world – seemingly undiminished by the events in Paris and Brussels
- Partially as a result, the European Court of Justice invalidated the EU-US Safe Harbor arrangement under the EU Charter of Fundamental Rights
  - Other cross-border transfer mechanisms legally uncertain

PAI

Now

- 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
  - Additional EU actions required before final approval
  - Facing severe criticism by influential EU privacy officials
- The 1995 Data Protection Directive and the implementing national laws will be replaced by the much stricter EU General Data Protection Regulation, finally approved last week.

PAI

The EU's General Data Protection Regulation

THE GDPR

What is a Regulation and how is it different than the Directive they have today?

Regulation vs. Directive

- A **Directive** is an order from the EU to the 28 Member States specifying a result to be achieved but leaving to the national authorities the choice of form and methods
- A **Regulation** is a binding law directly applicable in all Member States – like a US federal law
  - Since no other implementing language, is normally more detailed that a directive
  - The GDPR has 261 pages

PAI

THE GDPR

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

Expanded Geographic Reach

- Of course, applies to European processing of EU personal information by European subsidiaries
- However, also applies to the processing of the personal data of EU residents by a controller or processor outside the EU where the enterprise is
  - Offering goods or services to the EU residents
  - Monitoring of behavior or profiling of the EU residents
- In this situation, the controller or processor may have to designate a representative in the EU

Expanded Subject Matter Reach

- Definition of Personal Information has been expanded
- For instance, it is now absolutely clear under the GDPR that an IP address, and any information related to that IP address, is Personal Information just like a name

Potential Monster Fines and Private Actions Transform Privacy Risk Profile

- Today, privacy enforcement relatively weak, no private actions and penalties minimal
- Under GDPR, private 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 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

THE GDPR

So what has changed in the way we have to operate?

Must Be Able to Accommodate New Rights Granted to Individuals

- Detailed Privacy Notices when Data Collected
- Stronger Access Rights
- Data portability
- Right to be forgotten
- Restrictions on profiling

Your Consent Regime May Change

- Consent, including implied consent, is a basis used by most companies for processing PI or transferring it across borders
- Use of Consent will become much more limited
  - Must be **freely given** (bargaining power), specific, informed and unambiguous
  - By a statement or clear **affirmative** action
  - Controller has burden of proof

Your Consent Regime May Change

- Written consent in a document that deals with other matters must be clearly distinguishable and must use clear and plain language or it is not valid
- Must be as easy to withdraw as to give
- Contract performance or provision of a service cannot be made conditional on consent, if the processing is not necessary to the performance

Your Record-Keeping Obligations Have Mushroomed

- Maintain extensive records of processing activities for controllers
  - Purposes for processing
  - Categories of data, individual, and recipients
  - Transfers (list of third countries where data will be sent)
  - Erasure periods
  - Security measures applied
  - Must be able to prove consent
- Requirements for processors not as extensive

You May Have to Appoint a Data Protection Officer

- Mandatory appointment
  - Where processing sensitive data on a large scale
  - Where conducting regular and systematic monitoring of individuals
- Good practice where not mandatory
- Where appointed align function's responsibilities with GDPR requirements
- Reporting structure and employment protection

You May Have to Conduct Privacy Impact Assessments

- Where intended processing is likely to have high impact on privacy
  - Data Protection Impact Assessment (DPIA) required and
  - Where DPIA shows high impact is likely (without mitigating factors) also must have a prior consultation with the DPA

Your Data Breach Processes Must be Modified for EU to Comply With Strict New Rules

- 72 hour period after awareness to notify Supervisory Authority
- No report required when unlikely to result in risk for rights and freedoms of individuals
- Notice to individuals without undue delay where high risk for rights and freedoms

You Must Implement Privacy by Design

- Must implement appropriate measures for ensuring that every data processing complies with principles of privacy by design and default
- Where controller obtains consent for certain data processing activities it must take all measures to ensure that impact on privacy is mitigated
  - Use pseudonimization
  - Limit access and data retention
  - Practice data minimization, etc.

PAI

Privacy of Children

- The default age for giving valid digital consent is set at 16 years in GDPR
- Parental consent required for digital transactions for those under age
- Variation by member state explicitly authorized
- Member states may set own national level as low as 13

One-Stop-Shop

- Ability for organizations with multiple locations across Europe to nominate a single member state DPA as lead regulator at the main point of establishment (where decisions about data processing are made)
- May be a headquarters location or data processing center
- Organizational structural changes may affect location of the “main establishment” resulting in securing a more favorable member state DPA as Supervisory Authority
- Many unknowns about how process will operate in practice and level of cooperation DPA will exhibit

PAI

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

Recommendations

- Don’t wait - get started now with a plan
- Review operations and determine whether you are subject to the GDPR and document the findings
- If not already available, document personal data handling – what you have, where it came from, and with whom it is shared
- Assess enterprise structure and consider any changes desirable in establishing your lead supervisory DPA
- Document the legal bases used today for processing, including transferring, European PII and consider whether there are better alternatives
- Assess your practices for seeking, obtaining, and recording consent to see if they will still pass muster

Recommendations

- Check the format and content of current privacy notices used in the EU and redraft text and implementing procedures to comply with new rules
- Review internal processes to meet requirements on individuals' rights, e.g.
  - What are the processes that must be put in place or modified to grant data subjects access to data
  - Is data in a standard format so that can be exported to another company
- Modify incident response programs to comply with the GDPR

PAI

Recommendations

- Implement a records system to address the various documentation requirements
- Establish privacy impact assessment checklists and procedures
- Appoint a Data Privacy Officer, if required or desirable
  - Duties
  - Resources
  - Reporting structure
  - Candidates

Recommendations

- Review customer-facing materials to comply with new notice requirements;
- Review and amend agreements with processors to make GDRP compliant
- Establish and install privacy by design and data privacy impact assessment processes

Recommendations

- Raise in-house awareness through training so all stakeholders understand the upcoming requirements and risks
- If you deal with children, review the processes used to verify ages and gain and document parental consent
- Modify privacy audit and review processes with the GDPR in mind

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