PRIVACY ASSOCIATES INTERNATIONAL LLC

Managing Global Teams: Selected Privacy Challenges

Robert L. Rothman

West Michigan World Trade Week Business Conference
May 10, 2017

Purpose of Presentation

- Address at a high level some of the more significant privacy challenges involved in managing global teams from the US
- Focus primarily on two areas:
  - Cross-border transfers of Personal Information
  - EU General Data Protection Regulation that comes into effect in May, 2018 and has a monster effect on how many American companies must deal with their global teams

Who is on the Team?
What are their nationalities?
How are they performing?
What's their next position?
Who will succeed them?

Cross-Border Transfers of Personal Information

- Many countries have laws – often criminal laws – that severely restrict the transfer of personal information over borders
- Laws of most countries around the world based on the current EU Data Protection Directive
- In the EU you must have a legal basis to collect, store or transfer personal data even domestically **PLUS** a legal basis to transfer information to countries with inadequate privacy laws – like the US
- This includes the kind of info on prior slide
- Privacy is also a subject matter taken up by works councils

PAI

Main Legal Bases for Corporate Transfers of EU Personal Information to US

- Data subject consents
- Transfer is made pursuant to standard contracts drafted by the EU (and registered with the government in many countries)
- Transfer is made pursuant to “binding corporate rules” approved by appropriate Data Protection Authorities
- Privacy Shield Certification by U.S. Data Importer

Managing Global Teams Will Become Significantly More Challenging Beginning May, 2018

THE GDPR

- General Data Protection Regulation
- As a Regulation it applies to all EU countries
- Significantly increases protections for persons in the EU and burdens on organizations

That sounds problematic, but my organization is American, why should I care?

Extraterritorial Reach

- Of course, applies to European processing of EU personal information by your European subsidiaries
- However, also applies to the processing of the personal data of EU persons by a controller or processor **in the US** where the enterprise:
  - Has EU subsidiaries
  - Offers goods or services to EU persons
  - Monitors the behavior of the EU persons (e.g. behavioral advertising)

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, EU 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
  - €20,000,000 for Ma & Pa Online Store
- Privacy carries new levels of organizational risk

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:** no unequal bargaining power, specific, informed and unambiguous
  - By a statement or clear **affirmative** action
  - Data 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 (cross-border requirements basically the same)
  - Erasure periods
  - Security measures applied
  - Must be unambiguous for regular PI and explicit for sensitive data
- Requirements for processors not as extensive

PAI

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
- 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 Supervisory Authority

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

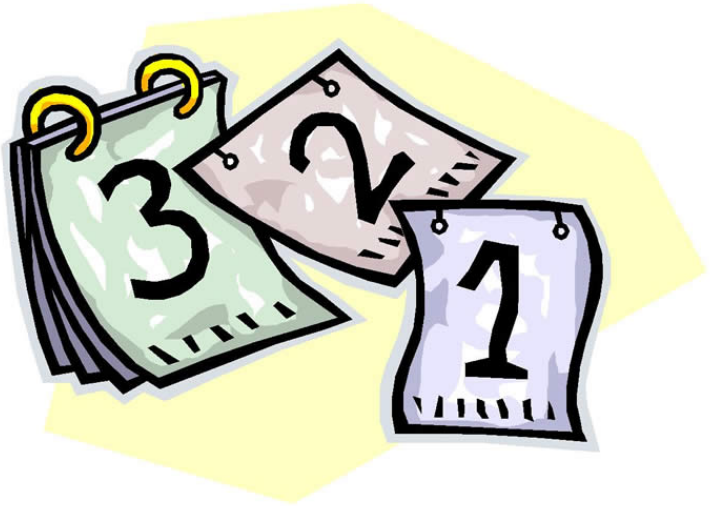
- 72 hour period after awareness to notify Supervisory Authority
- No report required when unlikely to result in risk for rights and freedoms of individuals
- Notice to individuals without undue delay where high risk for rights and freedoms

What About Managing Teams Outside the EU?

- Traditionally many countries around the world have followed Europe's lead
- Look for increasing number of countries to adapt GDPR rules, particularly those that are based on the current EU Data Protection Directive

Final Advice

If the global teams in your organization will be covered by the GDPR, start your compliance implementation efforts **<u>yesterday</u>**



PAI

Contact Information

Robert L. Rothman

Privacy Associates International LLC

rrothman@privassoc.com

www.privassoc.com

(248) 880-3942