WORLDWIDE ERC®

2018 Global Workforce Symposium

17 - 19 OCTOBER | SEATTLE, WA USA

General Data Protection Regulation Update

Tristan North, Worldwide ERC® Government Affairs Adviser - *Moderator*

Hank Roth, Associate Counsel/Chief Privacy Officer, Dwellworks®

William R. Tehan, General Counsel, Graebel® Companies, Inc.

Stephen Edwards, Worldwide ERC® Government Affairs Adviser, Europe

DESTINATION: SEATTLE

GDPR: the basics

- New rights for individuals – to be informed, access, rectification, forgotten, restrict processing, data portability , automated decision-making/profiling
- Legal basis for processing data
- Data Protection Officers
- Privacy Impact Assessments
- International transfers
- 72 hour breach notification requirement
- Maximum fine of €20m or 4% of global turnover
- Came into force in 25 May 2018

…Enforcement and case law is key

- Regulation – direct effect
- …but needs to be transposed and enforced nationally
- Over-reporting challenge
- Almost 43,000 complaints lodged under GDPR so far
  - Forced consent emerging as critical issue
  - Cambridge Analytica/Facebook
  - Fines levied locally

DESTINATION: SEATTLE

Future developments: EDPS

- Draft adequacy decision with Japan
- Territorial scope of GDPR
- Cross-border cases
- Annual review of Privacy Shield

Brexit

- Ongoing uncertainty as negotiations continue
  - Chequers plan
  - Adequacy
  - Hard Brexit

- Cautious optimism over data flows
- Future role of ICO subject of ongoing negotiation
- EU adequacy vs long-term flexibility (e.g. UK-India)

DESTINATION: SEATTLE

What's coming down the pike?

- E-privacy directive
- Copyright directive
- Free flow of non-personal data
- Data protection and competition/anti-trust
- Data protection in free trade agreements
- Data localization
- The US dimension?

Information Security and Data Privacy

- Recent Developments
  - E.U. General Data Protection Regulation (“GDPR”)
    - EU and member state data protection authorities are just beginning their work regarding the interpretation and enforcement of GDPR
    - Complaints and data breach notifications are being received but enforcement staff is not yet adequate to act upon them
    - Initial focus will likely be upon large data companies with audits, recommendations, and guidance documents preceding enforcement actions and imposition of fines
    - The EU Parliament adopted a non-binding resolution on July 5, 2018 calling for the suspension of the EU/US Privacy Shield unless the U.S. is fully compliant by September 1, 2018 – The annual review of the EU/US Privacy Shield is due on October 18-19, 2018

Information Security and Data Privacy

- Recent Developments
  - E.U. General Data Protection Regulation (“GDPR”)
    - Exercise caution in evaluating data breaches and determining which are reportable and how and when breach notifications are communicated to data protection authorities
    - Breach notification forms and required information on those forms are not uniform
    - Multiple notifications might be required if there is doubt as to the lead supervisory authority
    - Be careful with in-person communications since everything is “on the record”
    - Controllers need to report breaches within a short time period and that time period might be even shorter if the breach occurs at the processor level
    - Data Protection Addendums are very important and must contain the required provisions from Article 28 of the GDPR but negotiations are taking place on key issues

DESTINATION: SEATTLE

Information Security and Data Privacy

- Recent Developments
  - E.U. General Data Protection Regulation (“GDPR”)
    - Be prepared with a data breach response plan in advance of a breach
    - Detection and awareness are essential
    - Escalate potential problems to a designated response team
    - Provide timely notifications with appropriate content
    - Retain logs and other records
    - Perform remediation and identify lessons learned
    - Perform breach simulations and conduct audits and training
    - Stay current with ever-changing laws and regulations

Information Security and Data Privacy

- Recent Developments
  - U.S. Federal Cybersecurity Laws
    - The Cybersecurity and Infrastructure Security Act was passed by the House in 2017 and is awaiting consideration in the Senate – This Act would name the Department of Homeland Security as the lead agency for both infrastructure and civilian cybersecurity matters – The White House supports this legislation but others call for a new independent agency to handle this responsibility
    - The Department of Commerce issued a Request for Comments on September 25, 2018, on a proposed approach to consumer data privacy
    - Senior executives from Apple, Amazon, AT&T, Charter Communications, Google, and Twitter provided testimony before the Senate on September 26, 2018, in broad support of a comprehensive national law protecting consumer data privacy to replace a wide range of differing state laws

DESTINATION: SEATTLE

Information Security and Data Privacy

- Recent Developments
  - U.S. State Data Privacy Laws
    - All – U.S. state law data privacy laws and regulations contain different definitions and obligations and will likely be passed along by covered businesses to vendors by contract
    - California – Enacted the California Consumer Privacy Act on June 28, 2018, and amended that Act on September 23, 2018 – Effective as of January 1, 2020 – Applies to specified entities conducting business in California – Very broad definition of “personal information” – Grants consumers expansive rights to control the use of their personal information and imposes obligations upon covered businesses – Creates a private right of action, subject to a thirty (30) day notice period

Information Security and Data Privacy

- Recent Developments
  - U.S. State Data Privacy Laws
    - Colorado – Colorado amended data breach notification law and enacted data security requirements which were effective as of September 1, 2018 – Applies to "personal identifying information" of individuals residing in Colorado and requires that such information is protected when it is transferred to third parties
    - New York – New York's Cybersecurity Requirements for Financial Services Companies were adopted on March 1, 2017, and have phased effective dates over a two year period – Third party service provider security policies are required as of March 1, 2019

Information Security and Data Privacy

- Recent Developments
  - Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA")
    - Canada's Office of Privacy Commissioner (the "OPC") issued draft guidance on September 17, 2018, regarding new mandatory security and privacy breach notification requirements which will become effective on November 1, 2018 – breaches which present a "real risk of significant harm" must be reported to OPC and to relevant individuals
  - Brazil Data Protection Bill of Law
    - This bill was signed into law on August 14 and will become effective in 2020 – It is similar to the GDPR in structure and in anticipated enforcement
  - India
    - The Personal Data Protection Bill was issued in draft form on July 27, 2018, but has not yet been introduced for consideration.

DESTINATION: SEATTLE

Information Security and Data Privacy

- Recent Developments
  - Facebook Ireland and Max Schrems
    - On July 31, 2018, the Supreme Court of Ireland granted Facebook leave to appeal a lower court ruling allowing a challenge to Facebook's standard contractual clauses to be heard directly by the EU Court of Justice – The appeal will be heard within the next six months
  - French Data Protection Authority (the "CNIL")
    - On September 25, 2018, the CNIL published the results of its initial assessment of the implementation of the GDPR in France –The CNIL announced that it will publish new GDPR tools
- New Resources
  - Hunton Privacy Blog – www.huntonprivacyblog.com
  - TrustArc – www.trustarc.com

DESTINATION: SEATTLE

Who Must Comply With GDPR?

- GDPR applies to all organizations established in the EU
- For organizations established outside the EU, GDPR may or may not apply, depending on the circumstances
- A company based outside the EU is subject to GDPR if it either:
  - (a) offers goods or services to EU residents
  - (b) monitors the behavior of EU residents
  - Suppliers (processors) under contracts with RMC's or direct corporate clients may have to comply due to contractual obligations requiring GDPR compliance. Failure to do so becomes a breach of contract.

DESTINATION: SEATTLE

Processing

- Any operation or set of operations performed upon personal data or 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.
- * Art.4(2)

The Players under GDPR

CONTROLLER

- **A natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.**

***Art.4(7)**

PROCESSOR

- **A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Controller.**

*Art.4(8)

DESTINATION: SEATTLE

The Chain of Accountability

What is the chain of accountability under GDPR for the handling of the personal data of the corporate client's employees receiving relocation services?

- First, the personal data under GDPR must be that of an employee, transferee or assignee who resides (or is in) the EU (Data Subject).
- The corporate client, the RMC and all of the supplier's are in the chain and are accountable for the personal data in the hands of everyone with whom it is shared and everyone who processes the personal data from the corporate client to the RMC, from the RMC to the RMC's supplier and from the supplier to their suppliers.

How Does GDPR Impact Mobility? The Chain of Accountability (continued)

GDPR applies to anyone who:

- Collects and processes or transfers for processing the personal data of a Data Subject (residing or is in the EU)
  - Personal data means ANY information from which a person can be identified (e.g. name, location)
- Has employees residing in an EU member state (including multinational employers and EU employers who use relocation services)
- Sells (or offers) relocation products and/or services to corporate clients whose employees residing in the EU use the products or services (RMCs, downstream suppliers, etc.)
- Is a relocation service provider who provides relocation services directly to transferees, assignees, etc., who reside in (or are in) the EU regardless of where the supplier is located
- Is a sub-supplier who provides relocation services to suppliers who provide relocation services to transferees, assignees, etc., who reside in (or are in) the EU regardless of where the sub-supplier is located

DESTINATION: SEATTLE

What to be aware of: Impact on Your Business

- Worldwide application
- Big fines and penalties
- New data breach notification requirements
- DPOs, DPIAs, data mapping, reporting
- Privacy by design
- Data subject’s rights
- Responsibility for sub-processors

DESTINATION: SEATTLE

What to be aware of: Employers

- Consent not usable as a legal basis for processing employee data
- Intercompany transfers of data may not be compliant
- If GDPR applies, the collection, storage, and use of data must be compliant and data subject rights must be recognized

DESTINATION: SEATTLE

4 Keys to Ongoing Success

- Education and training
- Robust policies and procedure
- Minimization
- Updating privacy notices/privacy policies and contracts

DESTINATION: SEATTLE

Compliance Required

- Companies Failing to Comply: Fines Up to 4% of Total Global Gross Revenue, or €20 Million (whichever is greater)
- Controllers and now also Processors of Personal Data Must Provide
  - Appropriate security
  - Document processing activities
  - Include many new provisions in contracts with subordinate processors
- Complaints Alleging Violations Have Already Been Filed Against Several Large Tech Companies

How Do You Know What to Do?

Some Suggestions:

- RMC's consult with your large clients
- Suppliers consult with your RMC's
- Sub-Suppliers consult with your customers

1. Ask them what they expect you to do to help them to comply with GDPR in your capacity with them.
2. Do they see you as a Processor under the GDPR. If so what do they understand are your responsibilities to them regarding the handling of EU resident's personal data.
3. Determine you level of exposure.

DESTINATION: SEATTLE

Questions?