General Data Privacy Regulation: It's Coming… Are You Ready?

Presenters

Tristan North
Worldwide ERC® Government Affairs Adviser, Moderator

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

Hank A. Roth
Associate Counsel, DwellWorks, LLC

Lei Shen
Senior Associate, Mayer Brown

Outline of Session

- Provide overview of key concepts of GDPR
- Distinguish prior EU privacy concepts
- Discuss key definitions and scope of GDPR
- Consider GDPR in the context of relocation
- Present options for compliance and contracts
- Questions and answers

Background Information

- EU Data Privacy Directive (1995)
- EU/US Safe Harbor (2000)
- Court Challenges in the EU (2015)
- EU/US Privacy Shield (2016)
- Model Contract Clauses
- EU General Data Protection Regulation (2018)

Prior Concepts

EU/US Safe Harbor (2000)

- Permitted data transfers from EU to US
- Applied to data of EU citizens
- Self-certification process for US companies
- Safe Harbor invalidated in October 2015

Prior Concepts

EU/US Privacy Shield (2016)

- Contract provisions for onward transfers
- Right to correct data
- Applies to downstream data transfers
- Right of data subjects to opt-out
- Subject to ongoing legal challenges

New Concepts

EU General Data Protection Regulation (2018)

- Applies to EU residents, not just citizens
- Applies to monitoring of behavior
- Applies to controllers and processors
- Data mapping and Data Protection Officer
- Significant penalties for non-compliance

Employee Relocation Scenario

- Client retains RMC
- RMC initiates Transferee
- Client and Transferee provide PII to RMC
- RMC retains Vendors to provide services
- RMC needs to provide PII to Vendors
- All parties need to handle PII per GDPR

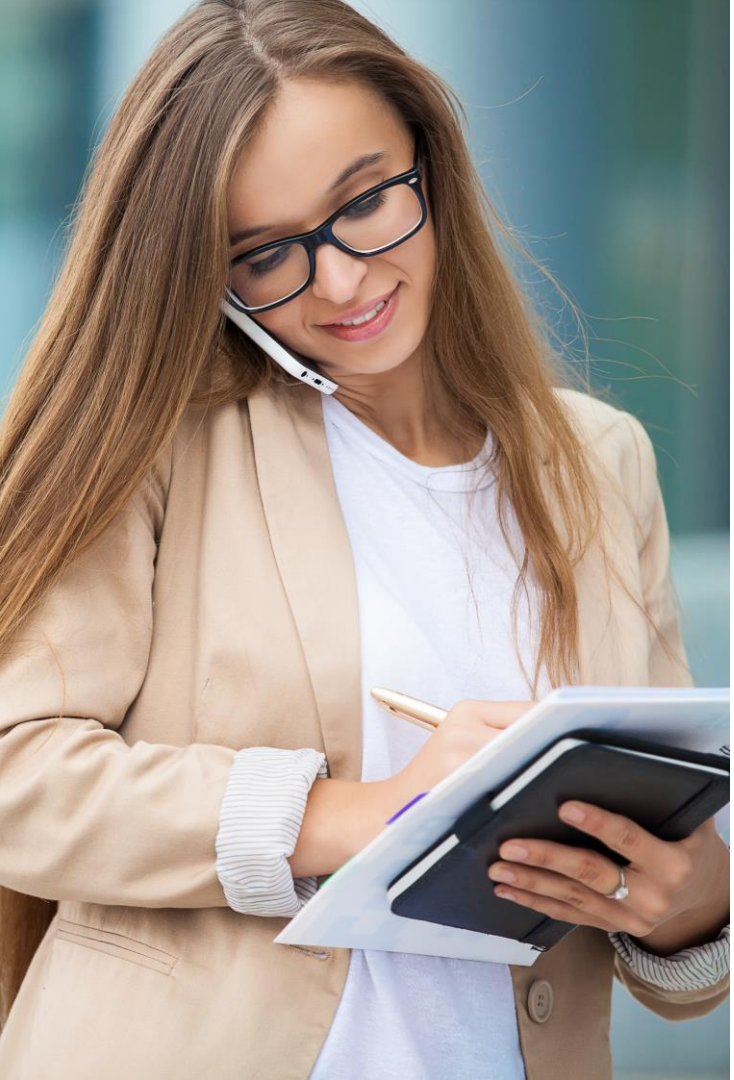
Desired Outcomes

- Compliance with EU statutes and regulations
- Compliance with contractual obligations
- Pass due diligence standards
- Downstream contracting with vendors
- Successfully pass future audits
- Establish framework for global compliance

Personal Data

Also referred to as PII, personal data means any information relating to an identified or identifiable natural person **("Data Subject");** a Data Subject is one who can be identified, directly or indirectly, in particular by reference to **an identifier** such as a name, an identification number, **location data**, online identifier or to one or more factors specific to the physical, physiological, **genetic**, mental, economic, cultural or social identity of that person. * **Rec.26; Art.4(1)**

* These Definitions will determine whether, and to what extent, the GDPR affects your business activities



Sensitive Personal Data

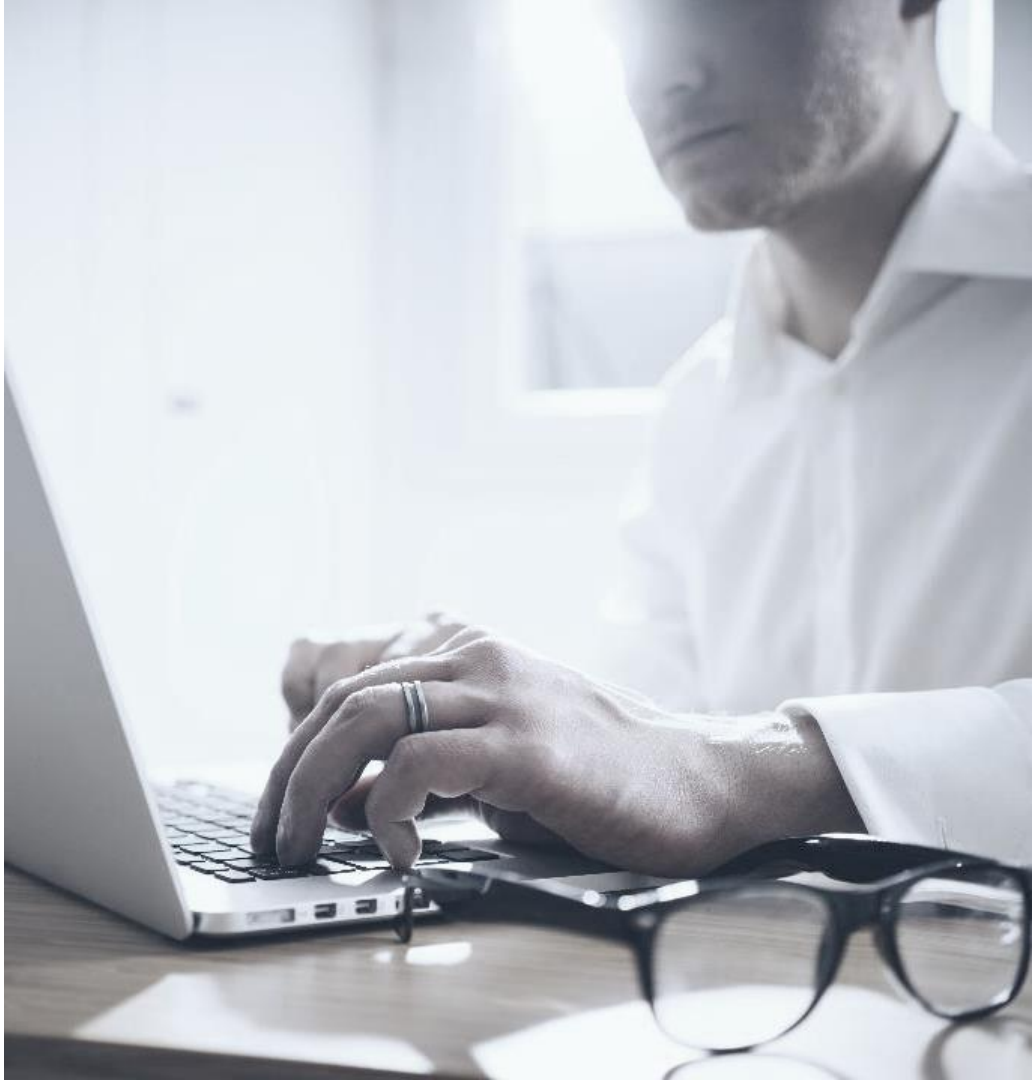
Personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

*** Rec.10, 34, 35, 51; Art.9(1)**

Processing

Any operation or set of operations performed upon PII or sets of PII, 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)



Controller

The 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)

Who must comply With the GDPR?

- **A company established in the EU is subject to the GDPR**
- **A company based outside the EU is subject to the GDPR** if it either: (a) offers goods or services to EU Data Subjects; or (b) monitors the behavior of EU Data Subjects.
- **A processor** that processes EU personal data for the above.

Who must comply with the GDPR specific to relocation?

Anyone who collects and processes or transfers for processing the **PII** of a Data Subject (residing in the EU) and:

- Has employees residing in an EU Member State (Including Multinational employers and EU employers who use relocation services)
- Sells relocation products and/or services to corporate clients whose transferees or assignees who reside in the EU use the products or services (RMC's, downstream suppliers, etc.)
- Is a relocation service provider who provides relocation services directly to transferees, assignees etc. who reside 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 the EU regardless of where the sub-supplier is located

In the Relocation industry - Who is your Customer when it comes to the handling of PII under the GDPR

A. If you are a corporate client - your customer is your employee using relocation services.

B. If you are an RMC - your customer is your corporate client using you to deliver relocation services to that client's employees.

C. If you are a supplier in the RMC's supply chain your customer is the RMC who was retained by the corporate client to deliver relocation services to its employees using relocation services.

D. If you are a sub-supplier to the supplier in the RMC's supply chain… you get the picture

The Chain of Accountability

What is the chain of accountability under GDPR for the handling of the PII of the corporate client's transferees and assignees receiving relocation services? First, the PII must be that of a transferee or assignee who resides in the EU (Data Subject).

The corporate client, the RMC and all of the suppliers in the chain are accountable for the PII of transferees or assignees in the hands of everyone with whom it is shared and are accountable for the processing of the PII from the corporate client to the RMC, from the RMC to the RMC's supplier and from the supplier to their suppliers.

The prior definition of Processing includes almost everything from receiving the PII to storing it, using it to deliver the services, transferring it for further processing, returning or "destroying" it.

The Chain of Accountability (Part 2)

We are also accountable to the Data Subject with regard to a new set or requirements called the Data Subject's Rights. These rights include our obligation to timely respond to any objection to the processing of their PII, providing access to their PII without a fee, amending it, having you erase data (The "Right To Be Forgotten"), change it, delete it, transfer it to another service provider (called "Data Portability"), assuring the security of it or returning it **and the right to object to use of their PII for direct marketing purposes**. At every step it must be handled securely.

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 PII.

3. Determine you level of exposure.

Cross-Border Rules Regarding Onward Transfers of PII

1. Rules are applicable to both intercompany transfers and to transfers to downstream suppliers.
2. We routinely share PII.
3. We share it in order to provide the services and products that we have been retained to deliver in the process of a relocation.
4. We share it with our affiliates on an intercompany basis for Processing purposes all over the world.
5. We share it with our downstream suppliers on an intercompany basis for Processing purposes all over the world.
6. GDPR applies to all of these onward transfers if they involve the transfer of PII of a Data Subject (see prior definition)

Cost Factors

GDPR Spending Projections:

- **83%** of companies surveyed expect to spend at least $100,000

The bigger the company the bigger the spend:

- **25%** of companies over 5,000 employees expect to spend over $1 million
- **20%** of Companies between 500-1000 employees expect to spend less than $100K
- Most surveyed indicated they needed help from outside resources

Source: TrustArc Inc - Benchmarking Your GDPR Compliance: Will You Make the Grade 2017

Where are you relative to Preparedness for GDPR?

About 40% are working on a preliminary plan (a few have not even started a plan)

About 60% Have a plan but most have not started implementation

*** Preparedness regardless of company size (Range – minimum 500 employees up to more than 5,000 employees) – Recent Survey July 2017 TrustArc Inc.**

Compare your Current Practices to the GDPR Requirements

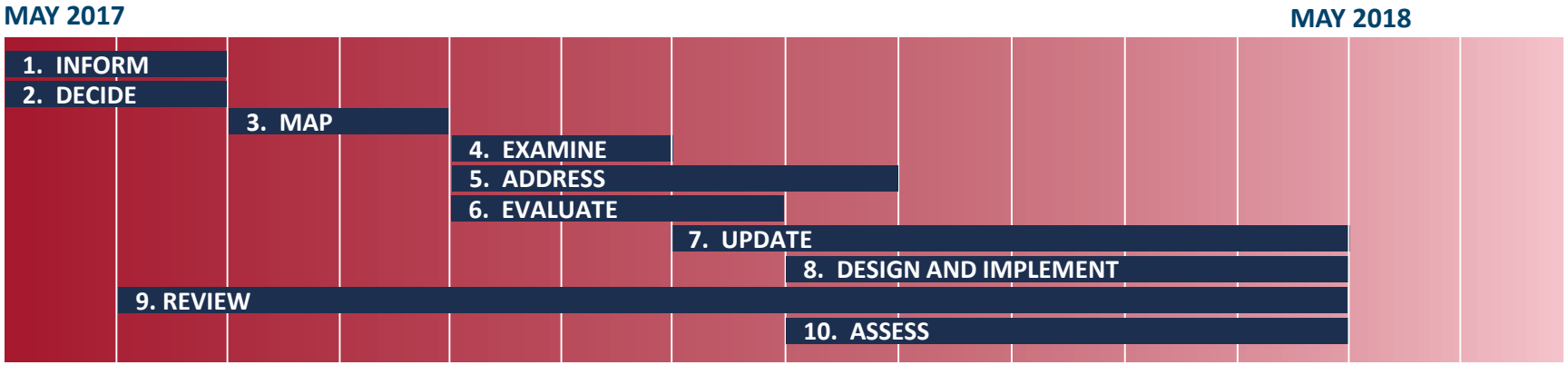
You need to compare your current practices against a comprehensive list of the requirements, including the following areas:

- **Right to Use** – Does your use the personal data only for the limited purposes that it was collected? Does your company get the right consent for its data processing activities? Do you map your data processing?
- **Data Breach Readiness and Response** – Is your company ready to respond to data breaches according to the GDPR's requirements? Do you have an data breach response plan in place?
- **Review Your Vendor Agreements** – Do your vendor agreements comply with the new GDPR requirements?
- **Assess Your International Transfers** – Are the international transfers of personal data being conducted by your business compliant with GDPR requirements?

Compare your Current Practices to the GDPR Requirements

- **Individual Rights & Remedies** – A key change under the GDPR is the expansion of individual rights (e.g., right to data portability). Because of this expansion, companies' existing policies, processes, and procedures must be reviewed. In some cases technological changes will need to be made.
- **Privacy Program Management** – Do you need to have a DPO? Do you perform DPIAs or incorporate privacy by design?
- **Security in the Context of Privacy** – What technical and procedural measures are in place and designed to protect your company's personal data?
- **Transparency** – How does your company disclose its data handling practices to data subjects? Do those need to be updated to comply with GDPR?
- **Bundling is Abolished** – Does your company provide any service that is conditional upon the individual giving consent for their data to be used for non-essential purposes such as marketing? This practice is banned under the GDPR.

Example GDPR Preparation Plan



1. **Inform** your leadership; formulate a plan
2. **Decide** whether a data protection office should be appointed and a data protection framework created
3. **Map** personal data that your organization is processing
4. **Examine** results to determine which of your data processing activities and business units must comply with GDPR
5. **Address** risks identified in any data processing activities
6. **Evaluate** grounds under which personal data is being processed
7. **Update** your data governance policies and procedures
8. **Design and implement** new compliance systems to comply with GDPR
9. **Review** supply chain contacts to endure that your service providers will comply
10. **Assess** any international transfers of personal data being conducted by your business

Key Change: Processor Obligations

Current Requirements (under the Directive):

- Controller (e.g., corporate client) has primary obligation to comply
- Controller must have written contract in place with processor that meets certain requirements
- Controller liable for breaches by data processor

Under the GDPR:

- Processors (e.g., RMC) will have direct obligations and liabilities under the GDPR
  - Cooperating with supervisory authority
  - Implementing security measures
  - Maintaining records of processing activities
  - Notify controller in the event of a data breach
  - Comply with cross-border data transfer requirements
- Enforcement by DPAs for breaching its obligations

Key Changes for Vendor Agreements under GDPR: Overview

Current Requirements (under the Directive):

- Only act on controller's instructions
- Implement appropriate technical and organizational security measures

Under the GDPR:

- Retains Directive's contractual requirements
- Also adds several new contractual requirements
- Most third party agreements will require some modifications
    - RMCs and subcontractors of any tier should be prepared for these changes

Updating Vendor Agreements: Required Provisions

Contract must address:

- Subject matter and duration of processing
- Nature and purpose of processing
- Type of personal data and categories of data subjects

- Obligations and rights of controller
- Process only on documented instructions from controller
- Duty of confidentiality
- Implement appropriate technical and organizational security measures
- Sub-processing restrictions
- Assistance to enable controller to comply with data subject requests (e.g., right to data portability)

Updating Vendor Agreements: Required Provisions (cont.)

Contract must address (cont.):

- Assistance to enable controller to comply with its obligations in Articles 32 to 36 (e.g., security, DPIAs, data breach, consultation, etc.)
- Data breach notification requirement
  - Processor must notify controller without undue delay in the event of a data breach
  - Compare to U.S. data breach notification obligations
- Deletion or return of data
- Record keeping
  - Make available information to demonstrate compliance with its processing obligations
  - Allow for and contribute to audits

Updating Vendor Agreements: Provisions to Consider

- Definitions
- Direct processor obligations
  - Record keeping
  - Cross-border data transfer requirements
  - DPO requirement
- Data protection by design
- If applicable, Privacy Shield onward transfer requirements
- Indemnities, limits of liability, and other similar clauses to address new risks