MAYER·BROWN

GDPR is coming in 108 days: Are you ready?

6 February 2018

Charles-Albert Helleputte

Partner, Brussels

+32 2 551 5982

chelleputte@mayerbrown.com

Diletta De Cicco

Legal Consultant, Brussels

+32 2 551 5974

ddecicco@mayerbrown.com

Welcome

- You were invited by Leadership Academy, ESAE or Mayer Brown to attend today's event
- In order to register to the event, you sent an email to one of the organisations with your contact details

❓ What should have happened between Leadership Academy, ESAE and Mayer Brown?

❓ What happens now?

The Mayer Brown Privacy Team will use your contact details to invite you to the next Privacy event

You are not a member of Leadership Academy/ESAE. You receive an email with the invitation to the next Leadership Academy/ESAE event

You exchange your business card with the Partner of the Mayer Brown Tax Team.
Next week you receive an email inviting you to an informal meeting with the team

MAYER·BROWN

Intro Quiz

- Most of you in the room are already subject to Data Protection law, do you know which one?
- Are you complying?
- What do you think are the main aspects of compliance today?

Agenda

1. The New Privacy Framework
2. Legal Basis for Processing
3. New Data Governance Measures
4. Transfer of Personal Data
5. GDPR Compliance for Trade Associations
6. Q&A

The New EU Privacy Framework

- The GDPR introduces new rules for data processing activities:
  - **Directive *vs*. Regulation** - Introduction of a single set of rules applying to all Member States
  - **Updating EU privacy law -** GDPR introduces rules in line with with new technologies

The New EU Privacy Framework

- The GDPR introduces new rules for data processing activities:
  - **New enforcement measures:** Fines up to 20 million euros or 4% annual worldwide turnover (whichever is the highest)
  - **Extraterritoriality principle:** GDPR will also apply to organisations based outside the EU if they target or monitor EU individuals – Not a game changer for most of you

❓ Can a US-based Working Group Member claim the application of the GDPR?

EU Privacy Law : Key Concepts

Personal data

Any information relating to an identified or identifiable natural person

Processing

Any operation or set of operations performed on personal data or on sets of personal data

Data controller

Natural or legal person that determines the purposes and means of the processing of personal data

Data processor

Natural or legal person, that processes personal data on behalf of the controller

Data Protection Principles

8 core Data Protection principles

- Transparency
- Fairness
- Lawfulness
- Purpose limitation
- Security
- Integrity
- Quality
- Data minimisation

Legal Basis for Processing

- Need to rely on specific legal grounds to process Personal Data:
  - Consent
  - Contractual necessity
  - Legitimate interest
  - Vital interest
  - Public interest
  - Compliance with legal obligations

❓ Are all of those new?

❓ Can you identify which one is the most affected by GDPR?

Legal Basis for Processing: Consent

- Threshold for valid consent significantly increased
  - Consent must be freely given, specific, informed and unambiguous
  - Need for a clear affirmative action
  - It must be recorded
  - It must be unbundled (clearly distinguished from other matters)
  - Could be withdrawn "at any time"

? In which cases could you rely on consent?

IN PRACTICE

If you rely on consent, when requiring individuals attending conferences or events to fill in a form and provide his/her data during the registration, provide a tick-the-box option or specific statement required to demonstrate acceptance of the proposed processing

Legal Basis for Processing: Necessary for the Performance of a Contract

- Controller must conduct a necessity test:
  - Controller cannot process information that is not necessary for the purposes of the contract
  - Need for a close and substantial connection between the data processing and the purposes of the contract

IN PRACTICE

Relevant if you need to process you employees' personal data to provide them with the payment of their salaries

Legal Basis for Processing: Legitimate Interest

- Personal data may be processed if the controller has a legitimate interest in processing the data AND if the legitimate interest is not overridden by the rights or freedoms of data subjects
- The assessment is carried out on a case-by-case basis

? Where else could you use this legal ground?

IN PRACTICE

Legitimate interest could include processing for direct marketing purposes. However always ask yourself:

What is the purpose of the processing and why is it important to you?

Is there another way of achieving the identified interest?

What are the rights and expectations of the data subjects?

Data Subject's Rights

- **Right to rectify**: data subjects have the right to ask for correction when data is inaccurate or incomplete
- **Right to object**: individuals have the right to object to the processing, for example if based on legitimate interest
- **Right to restrict the processing**: data subjects have the right to restrict the processing of their personal data in some specific circumstances
- **Right of access**: data subjects can ask for confirmation that their data is being processed and to access the data
- **Right to be forgotten**: a data subject has the power to ask the erasure of his/her personal data by the data systems (in specific circumstances)
- **Right to data portability**: data subjects may ask for personal data to be transferred directly from one controller/processor to another

New Data Governance Obligations

Impact Assessment

- Organisations are required to map their processing activities and undertake data protection impact assessments for higher risk processing

Privacy by Design

- Businesses must now take a proactive approach to ensure that an appropriate standard of data protection is the default position taken

Record of Processing

- Organizations have to demonstrate that their processing activities comply with GDPR, meaning that controllers will need to keep detailed records of the processing activities they carry out

? Which one do you think is the most relevant for you?

MAYER·BROWN

New Data Governance Obligations

Data Protection Officer

- Public authorities and organisations that carry out intrusive processing will have to formally appoint a Data Protection Officer

Data Breach Notification

- When a breach happens, the relevant European DPA must be notified without undue delay and, where feasible, within 72 hours. The individuals affected may also have to be notified

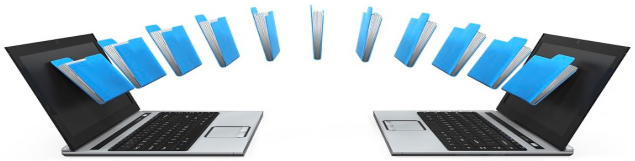
MAYER·BROWN

Transfer of Personal Data Outside the EEA

- Transfers of personal data outside the EEA are in principle excluded
- Transfers must be based on a legal transfer mechanism:
  1. Adequacy decisions
  2. Appropriate safeguards, including: Standard contractual Clauses ("SCCs"), Binding Corporate Rules ("BCRs"), etc.
  3. If (1) and (2) are not available, transfers can be based on derogations, e.g., explicit consent, contractual necessity, etc.

IN PRACTICE

If you rely on a service provider based outside the EEA in order to send invitations to events or newsletters, you must identify a specific legal transfer mechanism to transfer personal data



? But you are an EU-based association, why is this relevant?

Preparing for GDPR: A Practical Approach

MAYER·BROWN

GDPR Compliance for EU Trade Associations

1. Inform Your Leadership, Formulate a Plan
2. Map the Personal Data that Your Organisation is Processing
3. Decide Whether a Data Protection Officer Should be Appointed
4. Review the Grounds Under Which Personal Data is Being Processed
5. Draft or Review Information Notices
6. Update Your Data Governance Policies and Procedures
7. Review Your Contracts with Third Parties

Step 1 : Inform Your Leadership, Formulate a Plan

- Make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR

Provide a preliminary assessment of the application of the GDPR to your organisation

Ask external advisors to brief your organisation at the next board meeting

Draw up a high-level framework of the GDPR requirements that must be put into operation

MAYER·BROWN

Step 2: Map Your Personal Data

What do I need to "map"?

- Type of data and any classification
- Location of data
- Form of collection (or how it is obtained)
- Purposes of the collection and processing
- Details on storage (including where stored and who manages the system; whether there are back-ups)
- Encryption and destruction schedule
- Transfers and disclosures between business and third parties

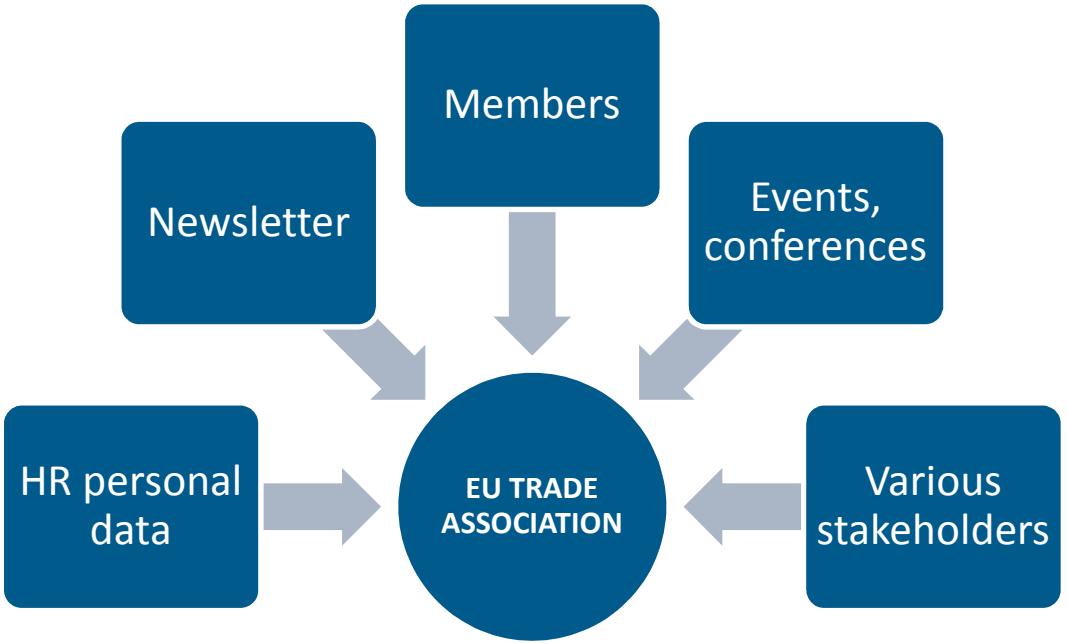
How do I "map" it?

- Gather information
  - Make a plan
  - Identify and review relevant policies
  - Involve key actors (HR, Communication, IT, etc.)
  - Ensure mapping is ongoing
- Make it visual (i.e., a *map*)
- Identify any gaps

EU Trade Associations Data Mapping Exercise

Data processing activity	Categories of personal data	Data subjects	Data collection method	Data processing purpose	Data are shared internally	Data are shared externally	Safeguards
Members							
Newsletter							
Events, conferences							
HR data processing							
Stakeholders							

EU Trade Associations Data Mapping Exercise



MAYER·BROWN

Step 3: Appoint a Data Protection Officer?

- Decide whether it is required under the GDPR to appoint a data protection officer
- Or your Members will decide for you...

Step 4: Review the Grounds for Processing

- On the basis of the information gathered during the data mapping exercise, review the legal grounds on which you rely on in order to process personal data
- Consider:
  - The purposes of processing (if you collect personal data for one purpose, you cannot use it for another incompatible purpose)
  - The context in which you collected the personal data – in particular, your relationship with the individuals and what they would reasonably expect
  - The nature of the personal data
  - The possible consequences for individuals of the new processing; and
  - Whether there are appropriate safeguards in place

Step 4: Review the Grounds for Processing

- **Do you always need consent?**
  - Representatives of member companies
    - When you send emails related to the working group they are part of (reports, working papers), you could rely on legitimate interest, but a STRICT TEST APPLIES!
    - When you plan to send emails not related to their specific working group, consider other legal basis (e.g., consent)
  - Individuals attending your organisation's conferences and events
    - When you send follow-up emails to people attending your events, you could rely on the legitimate interest ground, but a STRICT TEST APPLIES!
    - If you would like to invite them to other events, you should ask their consent!

Step 4 : Review the Grounds for Processing

- **What happens to your old database?**
  - You would like to contact all the individuals already included in your database to ask their consent on whether they would like to receive your newsletter going forward
  - **Honda Motor Europe fined £13,000**
    - Honda sent an email to 289,790 contacts asking "*Would you like to hear from Honda*?"
    - Honda was trying to comply with GDPR: the email was sent in order to clarify how many of the subscribers would like to receive marketing emails going forward.
- **Key take-away**: Even asking for consent is classified as marketing and is in breach of the upcoming GDPR!

Step 5: Draft or Review Your Information Notices

- Transparency of processing requires controller to provide information notices
- Notice must be provided at the time data is obtained (POC) and must include:

- **Identity and contact details of the controller**
- **Details of representative and DPO (if any)**
- **Purpose and legal basis of processing**
- **Data storage period**
- **Details of data transfers outside EEA and safeguards**
- **Recipients**
- **Use of automated decision making or profiling**
- **Details of legitimate interests**
- **Rights of access and correction**
- **Right to withdraw consent**
- **Right of complain to DPA**
- **Right of object to data processing**
- **Right of data portability**

Step 6: Update Your Data Governance Policies and Procedures

Policies and procedures should be updated to detail how your organisation will practically comply with the new requirements

IT security policies	Retention and destruction policies	Data breach notification Policy	Data processing register	Procedures to respond to data subjects' requests

Step 7: Review Your Contract with Third Parties

- Controllers must use a high degree of care in selecting processors
- Contracts must be implemented that contain a range of information– e.g., data processed and duration, obligations such as data breach reporting, use of technical measures, audit assistance obligations, etc.
- Data transfer restrictions apply to controllers and processors. Controllers should review whether any of the third parties they share personal data with is located outside the EEA and ensure they have a legal transfer mechanism in place

IN PRACTICE

Many EU trade associations rely on external companies providing newsletter services

Look at their Terms and Conditions and consider whether signing a Data Processing Agreement is necessary : if something goes wrong, you will be liable under GDPR!

Questions? Please contact:

Charles-Albert Helleputte

Partner (Brussels)

T: + 32 (0) 2 551 59 82

E: Chelleputte@mayerbrown.com

Diletta De Cicco

Legal Consultant (Brussels)

T: +32 (0) 2 5515974

E:Ddecicco@mayerbrown.com

MAYER·BROWN


Thank you for your attention

Notice

- The material in this presentation is provided for informational purposes only and does not constitute legal or other professional advice. You should not and may not rely upon any information in this presentation without seeking the advice of a suitably qualified attorney who is familiar with your particular circumstances. Mayer Brown Practices assumes no responsibility for information provided in this presentation or its accuracy or completeness and disclaims all liability in respect of such information.
- Mayer Brown Practices is, unless otherwise stated, the owner of copyright of this presentation and its contents. No part of this presentation may be published, distributed, extracted, reutilized or reproduced in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication) except if previously authorized in writing.
- Mayer Brown is a global legal services organization comprising legal practices that are separate entities (the "Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe – Brussels LLP; two limited liability partnerships established in the United States, Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales; JSM, a Hong Kong partnership, and its associated entities in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership. The Mayer Brown Practices is known as Mayer Brown JSM in Asia.

MAYER·BROWN