MAYER·BROWN

Public Affairs Post-GDPR: What You Need to Know

12 June 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 PAC to attend today's webinar
- In order to register to the event, you sent an email to PAC with your contact details. You have provided PAC with questions for us to answer today

What should have happened (if anything) between PAC and Mayer Brown

What happens now?

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

Next week the Mayer Brown Privacy Team invites you to a meeting to present you our firm

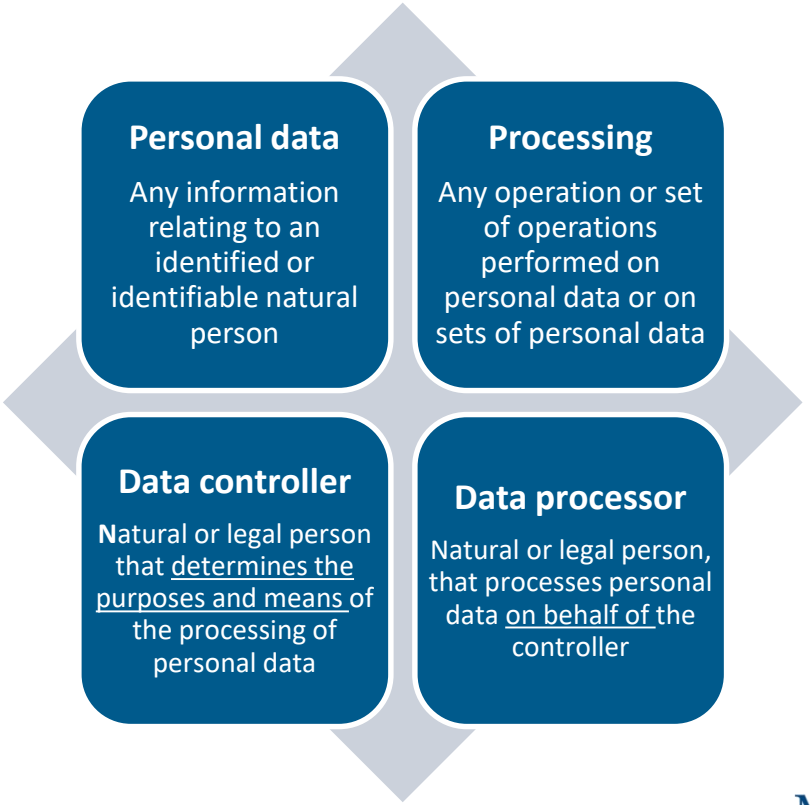
Agenda

1. The New Privacy Framework: snapshot
2. Data Governance Requirements and Why they are relevant to you
3. Practical Tips for Compliance
4. 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
  - **New enforcement measures:** Fines up to the greater of 20 million Euros or 4% annual worldwide turnover
  - **Extraterritoriality principle:** GDPR will also apply to organisations based outside the EU if they target or monitor EU individuals

EU Privacy Law : Key Concepts



MAYER·BROWN

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

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  - Could be withdrawn “at any time”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 PRACTICE

If you rely on consent, when requiring individuals attending 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 when organisations need to process employees' personal data to provide them with the payment of their salaries, or to process corporate expenses and reimbursements

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

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 of access: data subjects can ask for confirmation that their data is being processed and to access the data

Right to object: individuals have the right to object to the processing, for example if based on legitimate interest

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 restrict the processing: data subjects have the right to restrict the processing of their personal data in some 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

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

Data Governance Policies and Procedures … Are those for You?

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

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

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

A specific legal transfer mechanism should be identified if:

1. You rely on a service provider based outside the EEA in order to send marketing emails
2. You share personal data between different entities/departments of the same group

GDPR for Public Affairs: Practical Tips for Compliance

MAYER·BROWN

1. Can You Still Collect and Distribute Business Cards?

- **Receive and distribute business cards is not a processing activity <u>BUT</u>**
  - Processing starts when you are back at your desk and file the contact in your outlook database, excel spreadsheet, in an organised fashion on a paper file; AND
  - Data subjects (i.e., individuals) have rights
    - **Can you identify which ones by now? and when they kicks in?**

2. Do You Always Need Consent?

- **Do you always need consent?**
  - When working with stakeholders
    - When you contact and/or use details of individuals (e.g., institutions) to conduct advocacy activities, you may rely on legitimate interest, but a STRICT TEST APPLIES!
  - Individuals attending your companies' 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

3. Newsletter Footers Post-GDPR

- Newsletter sent to contacts

Pre-GDPR email footer (at best):

unsubscribe from this list

why did I get this? unsubscribe from this list update subscription preferences

Post-GDPR email footer:

When you subscribed to our newsletter, you provided us with your name and email address ("**Personal Data**") and you consented to receive our newsletters.

You can find more information on the above in our Newsletter Privacy Policy [link to the privacy policy]. You can also contact us at [insert email].

If you would like to unsubscribe from our newsletter, please follow this link [insert opt-out link].

4. Events' Consent Forms Post-GDPR

When you register to our event, you provide us with your name, email address, job title, name of the organisation. By clicking on the registration bottom, you consent to receive our communications with regard to this event.

By clicking one of the boxes below, you can choose whether you would like to receive our communication with regard to:

- ☐ our future events
- ☐ our newsletters

In order to organize event, we use Eventbrite, a U.S.-based event management website. We have taken steps with EventBrite to ensure that the transfer of your personal data to them complies with EU data privacy laws. You can find more information on the above in our Privacy Policy **[link to the privacy policy displayed on the website to be inserted].**

If you would like to contact us about the way we process your personal data, you can do so at **[insert email]**.

5. Are Re-Consent Emails an Option?

- **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

6. When Contracting 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.
- Speak to your procurement / legal / any relevant team(s) to make sure that you are not placing the company at risk

IN PRACTICE

When you rely on external companies to send newsletters, organise events, host your databases, run the recruiting process, etc. signing a Data Processing Agreement is necessary. If something goes wrong, you will be liable under GDPR

7. Post-GDPR Tranfers of Personal Data

- Data transfer restrictions also apply when you send EU personal data to entities or departments of the same group located outside of the EU
- In this case you should:
  - At the time of the collection, inform individuals that the data will be transferred
  - Ensure that there is a legal mechanism in place that covers the transfer of personal data

GDPR Dos and Don'ts

Dos

- Collect only the information you need to conduct a specific activity.
- Make information on what you do with personal data easily accessible to the public.
- Provide an easy way to withdraw consent and inform individuals on how to do that.
- Delete personal data if you don't need them anymore.
- Share personal data only if you have a reason for doing so and if you know there is a legal mechanism in place.
- If you have doubt about how to handle personal data, contact the person/team in charge within your organisation.
- Ensure you secure personal data appropriately (e.g., where possible keep paper files locked away and your desk clear).
- Factor personal data framework in everything you do.

Don'ts

- Don't assume people will be interested in everything you do (and hence that any outreach is legitimate)
- Don't use personal data from a different purpose from the one they were collected.
- Do not have vague terms in consent forms and privacy notices, they should be as granular as possible.
- Do not disclose personal data to an external organisation without first checking if the individual has been informed and, in some cases, consented.
- Don't email anyone who has asked not to be contacted, unsubscribed from a list, or opted-out in any other way.
- Don't fail to report subject access rights requests or breaches.
- Don't put the organization at risk (by sharing username and passwords, have business data on mobile devices, "spray and pray", etc.)

You don't need our consent!

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) 2 551 59 74

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