

General Data Protection Regulation and NGOs: Are you Ready?

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

24 April 2018







- You were invited by A4ID to attend today's event
- In order to register to the event, you registered with Eventbrite



What should have happened (if anything) between A4ID, Eventbrite and Mayer Brown?

Do you have any privacy expectations in that regard?

What is the impact of GDPR on NGOs daily activities?



You reach out to people you know are potential supporters of your actions to raise funds

Participants who are not one of your members attends one of your events. You use their contact details to invite them to your next event

During an event, you exchange your business card with one of the attendees. The next day, you use its contact details to inform him/her about your activities



1. The New Privacy Framework
2. Legal Basis for Processing
3. New Data Governance Measures
4. Transfer of Personal Data
5. GDPR Compliance for NGOs
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 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

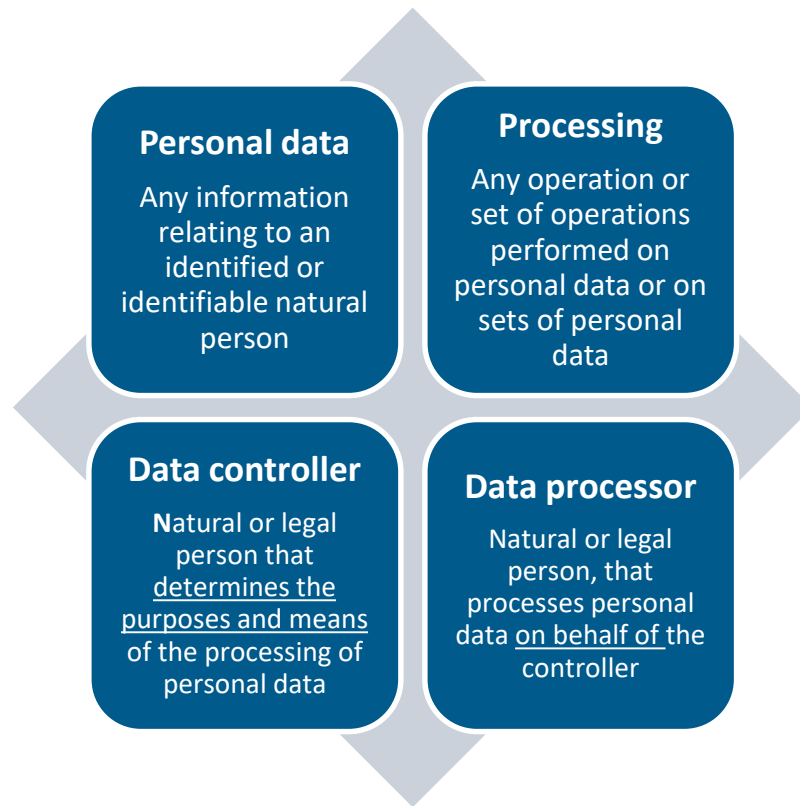


How will this affect your organisation?

The GDPR: extraterritorial scope



European Data Protection Directive 95/46 applies to:	General Data Protection Regulation 2016/679 applies to:
A data controller where it is established in an EU Member State <u>and</u> the data is processed in the context of that establishment	The processing of personal data in the context of the activities of a data controller or data processor established in the EU, <u>irrespective</u> of where the processing takes place
A data controller where it is not established in an EU Member State but is using equipment in an EU Member State for processing data otherwise than for the purposes of transit through that Member State	The processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU, where the processing activities are related to: <ul style="list-style-type: none">• The offering of goods or services to those data subjects; or• The monitoring of their behaviour in the EU





8 core Data Protection principles

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





- 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?



- 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 their 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



MAYER • BROWN



IN PRACTICE

- 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?

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?

Processing special categories of data



- **Sensitive data** = data on racial or ethnic origin, political opinions, religious or philosophical beliefs, sex life, sexual orientation, trade union membership, **genetic data**, health data, **biometric data**.
- They are granted a **higher level of protection**: need to rely on a specific legal ground (e.g., explicit consent for the data subject).




IN PRACTICE

Example


You are processing sensitive data when:

The data subject provides information on allergies during the registration process of an event


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

- Organisations 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?

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

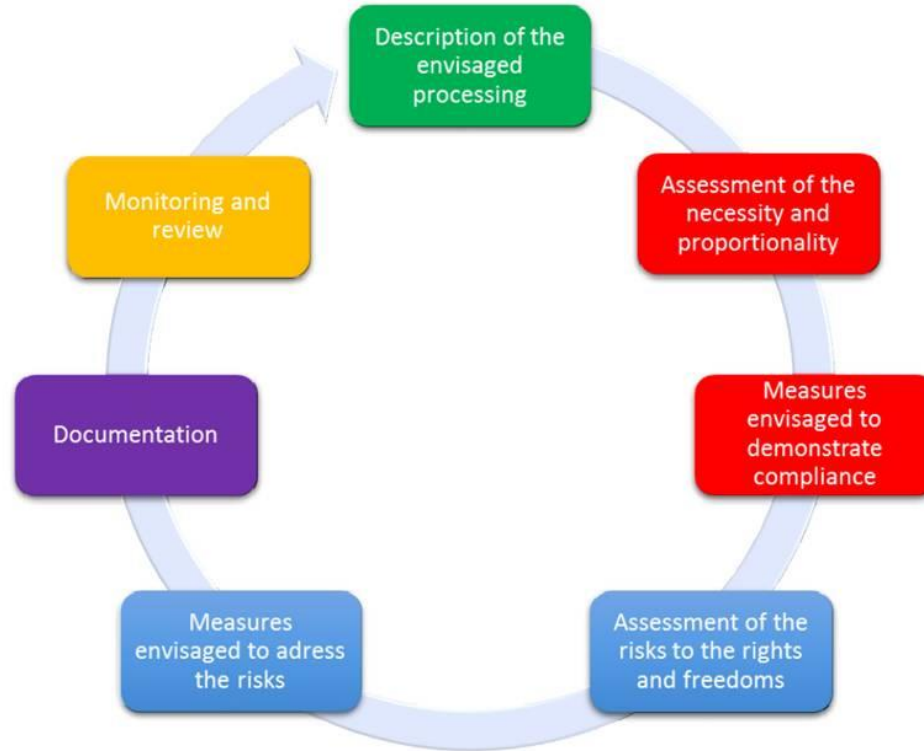
- When a breach happens, the relevant European DPA must be notified without undue delay and, where feasible, within 72 hours. The individuals affected may also have to be notified

Data Protection impact assessment



- “A DPIA must be conducted with respect to activities that are likely to result in a **high risk** to the rights and freedoms of the individuals concerned, particularly when using new technologies.
- These include activities that involve:
 - › Systematic, extensive evaluation of personal aspects of persons based on automated processing – i.e. profiling;
 - › The processing of sensitive personal data, criminal convictions and offenses;
 - › Systematic monitoring of publicly accessible areas on a large scale; or
 - › Data transfers outside the EU; etc.

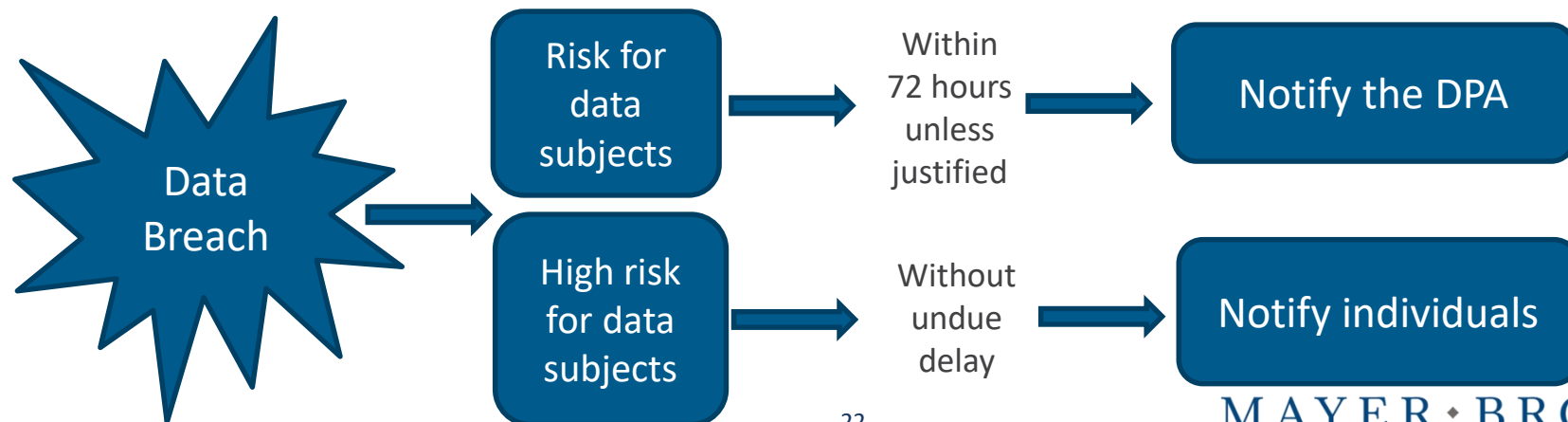
Data Protection impact assessment



Data Breaches notification obligations



- **Data breaches** = breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed
- Data processors must report personal data breached to data controller
- Data controller must maintain an internal breach register



Transfer of Personal Data Outside the EEA



IN PRACTICE

- 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.

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?



**KEEP
CALM
AND
COMPLY WITH
GDPR**

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

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							



Step 3: Appoint a Data Protection Officer?



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

Step 3: Appoint a Data Protection Officer?



Responsibilities of a DPO

- Monitor compliance with GDPR
- Assist with the production of DPIAs
- Pay particular attention to high risk processing
- Available for data subject concerns
- Cooperate with DPAs

Rights of a DPO

- Sufficient funding and access to perform the role
- Certain degree of autonomy
- Protected under the GDPR from unfair dismissal/termination in some cases
- Business must involve the DPO from the outset in all related issues

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 process data of your members, you could rely on legitimate interest, but a STRICT TEST APPLIES!
- When you process other data subject data, consider other legal basis (e.g., consent)

- › Individuals attending your organisation's conferences and events

- When you follow up 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

Data breach
notification
Policy

Retention
and
destruction
policies

IT security
policies

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

Most 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) 2 551 59 74

E: Ddecicco@mayerbrown.com

MAYER • BROWN



Thank you for your attention



- 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.