



G.D.P.R. FOR ASSOCIATIONS

Moderator: Danièle VRANKEN, Secretary General, FAIB

Presenter: Nicolas HAMBLENNE, Lawyer, KOAN Law Firm

Presenter: Laurent MASSON, Lawyer, DKW Law

Presenter: Thomas VAN GREMBERGHE, Company Lawyer, AGORIA

Presenter: Fabienne RAEPSAET, Lawyer, Claeys & Engels



Learner Outcomes

With this session, you will learn what your association can/should do in practice to be **GDPR-compliant by 25 May 2018.**





.AGORIA



- 1. Introduction to the legal background - EU Regulation - Cost - Timing - DPO;
- 2. Data mapping – Record; (updated 14.03.2018)
- 3. Consent – transparency;
- 4. Human resources aspects




The Challenge of Compliance to the GDPR

1. Introduction to the legal background - EU Regulation - Cost - Timing - DPO;
- Why should personal and sensitive data be protected?
 - Why regulate Data Protection at European level?
 - The cost of compliance v. the cost of non compliance?
 - Time left to achieve compliance?
 - Data Manager or Data Protection Officer (DPO)?
 - Where to start?



6th European Association summit 2018
8 & 9 March

Directive vs. Regulation




Data Protection Directive


- ✓ Old directive (1995) vs new technology
- ✓ Fragmentation and inconsistency due to 28 local interpretations
- ✓ Lack of compliance due to absence of enforcement / sanctions

➔

GDPR


- ✓ Adapt legal framework to the globalized digital society
- ✓ “One ring to rule them all”
- ✓ Increased rights for individuals
- ✓ Increased obligations for organizations
- ✓ Increased enforcement





6th European Association summit 2018
8 & 9 March

Sanctions



Up to 10M€ or 2% of worldwide turnover


For issues related to :


- Failure in **security of the processing**
- Infractions regarding to **privacy by design / by default**
- **Data Protection Officer**
- Failure to **notify a data breach**
- ...

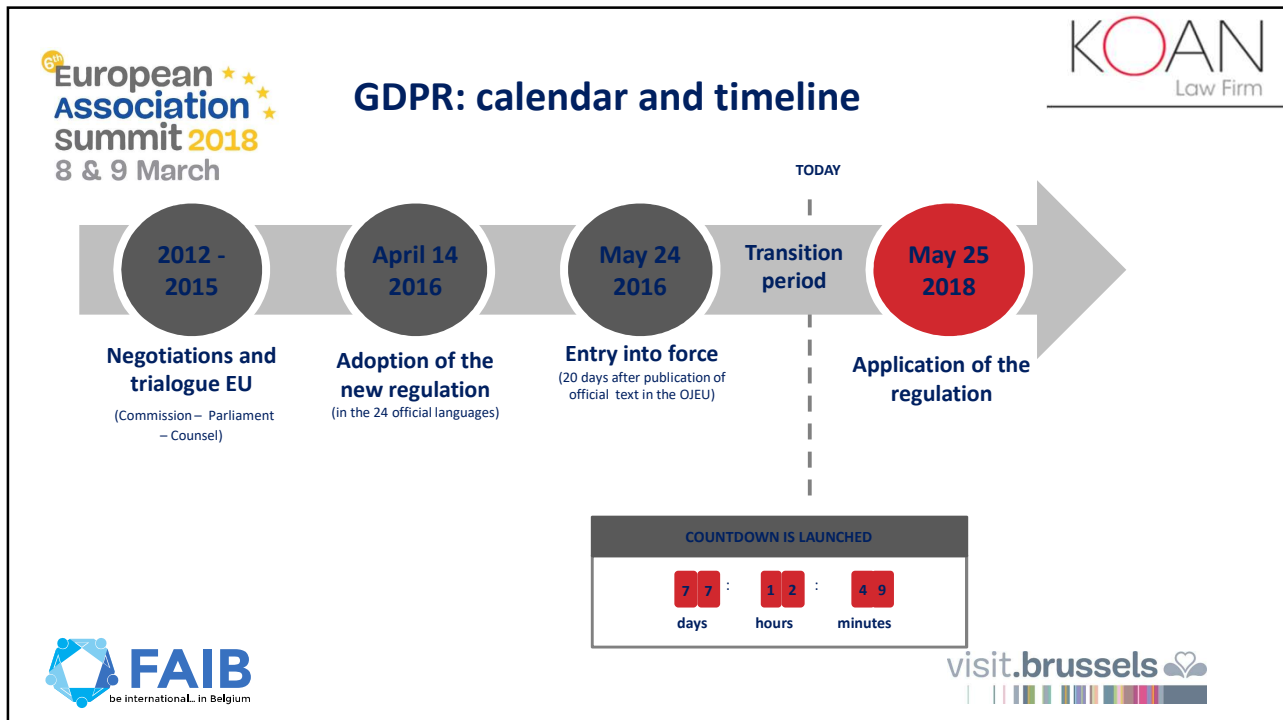
Up to 20M€ or 4% of worldwide turnover

For issues related to :

- **Sensitive data**
- **Transfers** of personal data
- Non compliance with a **supervisory authority's order**
- Issues regarding **data subject's consent**
- ...







6th European Association summit 2018
8 & 9 March

Data Protection Officer (DPO)

KOAN Law Firm

- **DPO : contact** for issues related to **data of a natural person**.
- **Main role** : being involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

Obligatory DPO for certain associations

- ✓ The processing is carried out by a **public authority or body**;
- ✓ The **core activities** consist of processing operations which require **regular and systematic monitoring** of data subjects **on a large scale**;
- ✓ The **core activities** consist of **processing** on a large scale of **special categories of data**.

FAIB be international. in Belgium

visit.brussels

Data Protection Officer (DPO)

Requirements

Expert level
Questions related to personal data (appropriate way and in due time)
Necessary resources (personal, time, financial means...)
Full autonomy (internal or external DPO)
No conflict of interests (cannot be a CEO, COO, CFO, CMO, ...)

Tasks

- ✓ Ensure conformity with the GDPR and an effective protection of data
- ✓ Develop, review and update data protection systems (IT, policies, etc)
- ✓ Inform, educate and advise the officers/and personnel
- ✓ Point of contact and cooperation with the supervisory authority
- ✓ + ...

2. Data mapping and Record

- Data mapping :
 - What? Complete overview of all data processing performed within the organisation
 - Why? Essential step prior to record
 - How? Key persons (IT, HR, ...)

2. Data mapping and Record

- Data mapping : identifying and mapping out all data flows.
- 5 « W » questions :
 - **What** categories of data are held?
 - **Who** « owns » the data, and who gets access to it?
 - **Why** : for what purpose are the data being held?
 - **Where** are the data being held?
 - **When** : for how long do you keep the data?

2. Data mapping and Record

- Data mapping :
 - Systematic and organised approach :
 - Appoint a project leader/team
 - Define a project plan : outline priorities/timeline/responsibilities
 - Gather relevant information from all departements of the organisation
 - Persons to be involved in data mapping exercise: CEO, heads of departments (HR, marketing, IT,...)

2. Data mapping and Record

- Records of processing activities: **who?**
 - Mandatory :
 - Enterprise or organisation employing **more** than 250 persons ;
 - Enterprise or organisation employing **fewer** than 250 persons a.o. if the processing is not occasional, or includes sensitive data.
 - Occasional : “occurring at irregular or infrequent interval”.
 - Ex of non-occasional processing : staff/ customer/supplied management
 - Recommended (by Belgian supervisory authority) : in any other situation → Accountability requirement

2. Data mapping and Record

- Records of processing activities: **why?**
 - Accountability requirement : each data processing must be GDPR compliant (article 5.2 GDPR)
 - Record will be requested by the supervisory authority
 - No record : administrative fines

2. Data mapping and Record

- Records of processing activities: **how ?**
 - In writing, including in electronic form
 - No imposed format
 - Models of record proposed by supervisory authorities
 - No mandatory language (but national language to be preferred)
 - Up-to-date
 - Retention : 5 year after the termination of the activity (Belgian supervisory authority recommendation)

2. Data mapping and Record

- Records: what ?

Contact details of the **controller** (and if applicable data protection officer)

Purposes of the processing
Ex: members administration, customers administration, staff administration, public relation activities,...

Description of the categories of **data subjects** (*ex: members of association, external providers, employees, stakeholders,...*) and **personal data** (*ex: identification data, data related to job qualification, schooling,...* ! Sensitive data!)

Categories of **recipients**
Ex: social secretariat, insurance companies,...

2. Data mapping and Record

- Records: what ?

If applicable,
transfers of personal
data to a **third
country** or an
international
organisation

General description of
the technical and
organisational **security
measures**

Contemplated time
limits for **erasure** of
the different
categories of data

Additional non mandatory information ?

- Method of collection;
- Location of data storage;
- Deletion method;
- **Legal basis** (consent, contractual obligation, legal obligation, legitimate interest,...);
- ...

3. Consent

- Informed consent
 - Intelligible and easily accessible
 - Clear and plain language
- Active
- Freely given – choice
- Clearly distinguishable from other matters
- Demonstrate !
- Right to withdraw consent at any time

I Agree

3. Transparency

Information and communication regarding processing activities



- Concise, easily accessible
- Intelligible, clear and plain language
- No formal requirements
 - ↔ CCTV
 - ↔ Employment law



General obligation ↔ informed consent

Much more information to be provided

- Identity + contact details DC / DPO
- Purposes + legal basis
- Recipients
- Retention
- Data transfer

- Data subjects rights
- Right to file a complaint
- *Right to withdraw consent*
- *Legitimate interest*
- *Automated decision making*

If data not obtained by data subject

- Personal data + source

3. Action plan

➤ Review and adapt consent mechanism

- Informed
- Layered approach
- Separate from other matters

I Agree

➤ Transparency

- Register as starting base
- Review and adapt
- Update
- Accessibility – layered approach
- Employment law - consequences



4. Human resources aspects

- **Personal data**

- Salary and personnel administration
- Job applicants, employees, contractors,...
- E-monitoring, track & trace, camera surveillance,...
- Record of presences
- Photo book intranet/internet
- Special categories of personal data

4. Human resources aspects

- **Data controller / Data processor**

- Payroll agency
- Recruitment agency
- Service provider
- Insurance company

6th European
Association
summit 2018
8 & 9 March

 lus Laboris Belgium Global HR Lawyers
Clays & Engels

4. Human resources aspects

- Lawfulness?
 - Performance of the employment contract
 - Compliance with a legal obligation
 - Employer's legitimate interests
 - Employee's consent?



6th European
Association
summit 2018
8 & 9 March

 lus Laboris Belgium Global HR Lawyers
Clays & Engels

4. Human resources aspects

- What is at stake?
 - Fine?
 - Damages?
 - Position of employment courts

