GDPR FINALLY BECAME REALITY

Antoine Druetz
Nicolas Hamblenne

FAIB
be international... in Belgium

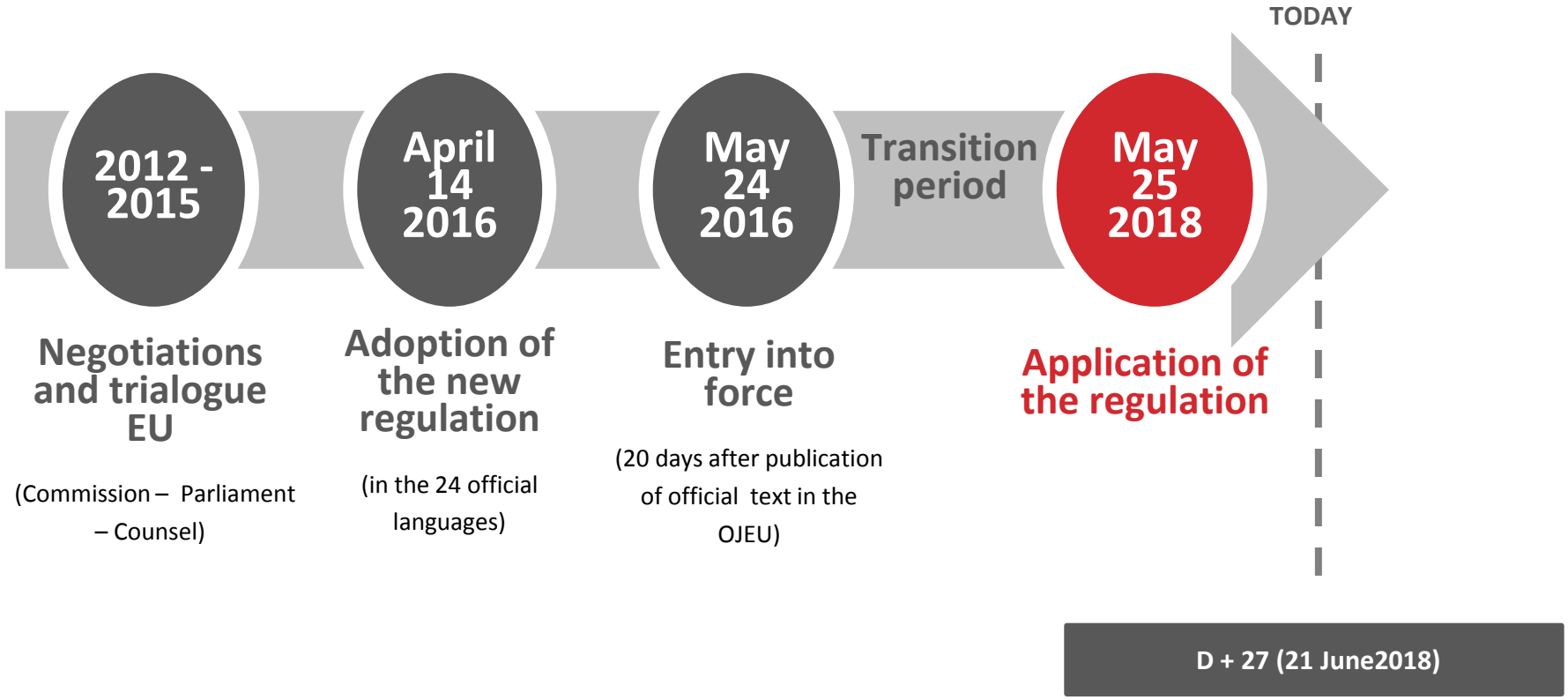
KOAN

TABLE OF CONTENTS

I. INTRODUCTION

KOAN

GDPR: calendar and timeline



II. PRIVACY
Concepts and Principles

KOAN

Legislative framework in Belgium

Belgian Privacy Act

***Act** of **8 December 1992** on the protection of privacy in relation to the processing of personal data.*

Data Protection Directive

***Directive** 95/46/EC of the European Parliament and of the Council of **24 October 1995** on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

General Data Protection Regulation (GDPR)

***REGULATION** (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of **27 April 2016** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

KOAN

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

KOAN

Different types of data

PERSONAL DATA

All information concerning an identified or identifiable physical person.

- Name
- Picture
- Phone number (personal/professional)
- Bank account number
- E-mailaddress
- IT (Addresses, IPv4, IPv6, Mac address, DeviceID, …)
- License plate

PSEUDONYMOUS PERSONAL DATA

Data that cannot be linked to a certain person without relying on additional information.

SENSITIVE PERSONAL DATA

- Medical file (genetic & health records)
- Fingerprint / iris scan (biometrical data)
- Judicial file
- Ethnic origine(race or origine)
- Sexual orientation (behaviour or preference)
- Political preference
- Religious or philosofical beliefs
- Trade-Union membership
- Criminal convictions and offenses / security measures.

ANONYMOUS DATA

Data that is neither personal, neither pseudonymous.

KOAN

Processing and relevant actors

PROCESSING

Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as

- collection, recording, organization,
- storage, adaptation or alteration,
- retrieval, consultation, use
- disclosure by transmission, dissemination,
- alignment or combination,
- blocking, erasure or destruction.

CONTROLLER

The **natural/legal person** which **determines the purposes** and **means** of the processing of personal data.

PROCESSOR

A **natural/legal person** which processes personal data **on behalf of the controller**.

KOAN

General principles

Legality	Each processing must be based on a legal basis	**Finality**	Specific, adequate and legitimate goal

Proportionality	▪ Precise, relevant and necessary (not excessive) data ▪ Exact and up-to-date data ▪ Reasonable conservation period

Security and confidentiality	▪ Access data protection (secured servers, passwords etc.) ▪ Confidentiality agreements

KOAN

General principles: principle of legality

6 legal bases in order to process personal data:

Consent

Necessary for the **execution of a contract**

Legal obligation

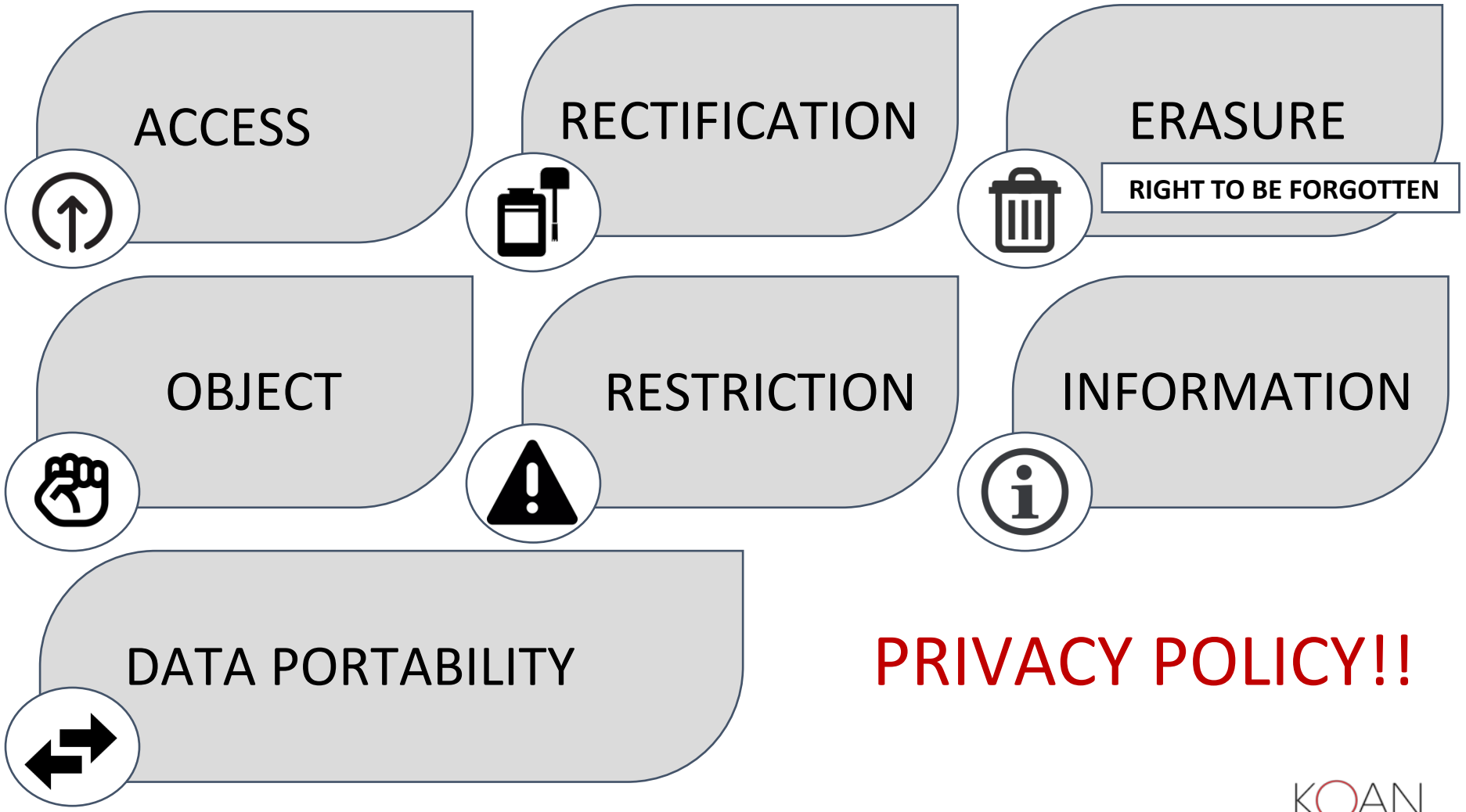
Protection of **vital interest**

Missions of **public interest** or exercise of **public authority**

Legitimate interest of the controller or third party

KOAN

DATA SUBJECT RIGHTS



PRIVACY POLICY!!

KOAN

Transfer of personal data abroad

TRANSFER

WITHIN the European Economic Area

→ **no obstacles**

TRANSFER

OUTSIDE the European Economic Area

↓

COUNTRY OUTSIDE EEA

WITH ADEQUATE LEVEL OF PROTECTION ?

YES:

WHITE LISTED COUNTRIES

(Switzerland, Andorra, Argentina, Guernsey, the Isle of Man, the Faroe Islands, Jersey, Israel, New Zealand and Uruguay)

→ **No obstacles**

NO:

USA: Binding Corporate Rules, EU Commission's model clauses, or EU-US Privacy Shield

Other countries: Binding Corporate Rules, EU Commission's model clauses

KOAN

III. GDPR : TOP 5 KEY ISSUES

I. Consent

II. Legitimate interest

III. Breach notification

IV. Accountability & Sanctions

V. Data Protection Officer (DPO)

KOAN

I. Consent

Consent for ordinary categories of data

- **Free**
- **Specific**
- **Informed**
- **Unambiguous**

Consent for special categories of data

Consent must be **explicit**
(not defined but stronger than 'ordinary' consent)

Parental consent for children aged between **13 and 16 years**

(Leeway for each Member State)

Examples:

Cookie banner (or cookie policy) on website

Explicit "opt-in" when registering a new account (user);

KOAN

II. Legitimate interest

Legitimate interest vs **legitimate expectation**

- Balance of interests (on a case-by-case basis)

(47) **The legitimate interests of a controller**, including those of a controller to which the personal data may be disclosed, or of a third party, **may provide a legal basis for processing**, **provided that the interests or the fundamental rights and freedoms of the data subject are not overriding**, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist **for example** where there is a relevant and appropriate relationship between the data subject and the controller **in situations such as where the data subject is a client or in the service of the controller**. (…)

The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

Important for **Marketing purposes**

- Business cards
- Opt-out
- Keep track of information

KOAN

III. Breach notification

When ?

Any **data breach must be notified** to the supervisory authority by the data controller **within 72 hours**

Who ?

Notification to the data subjects "***without undue delay***" if the breach could create a "***high risk***" to them

Exceptions

No notification to the privacy authority if the data breach **is not "likely to cause any risk to the rights and freedom of the data subjects"**

No notification to the data subject if the data breach **is not "likely to cause a high risk to the rights and freedom of the data subjects"**

Notification in chain

The **processor** should **notify any data breach to the data controller** who will on his turn notify the privacy authority

KOAN

IV. Accountability…

- **Much heavier** than in the Directive (1995)
- Real need to **demonstrate compliance** with the GDPR
  - **Adoption of policies**
  - **Regularly review** and **assess** data protection **measures**
  - Adoption or approval of established **codes of conduct**
  - **Keep records** of all processing activities

No record of processing activities required (exception):

- **Exception** for companies with < 250 employees **provided that** :

  (i) the processing is **not likely to give rise to a risk** to the rights and freedoms of the data subjects;
  (ii) the **processing is occasional**; and
  (iii) **no sensitive data** are processed.

KOAN

… and 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**
- …

KOAN

V. Data Protection Officer (DPO)

- **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.

Mandatory DPO for certain organisations

- ✓ 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**.

KOAN

V. 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
- ✓ + ...

KOAN

IV. COMPLIANCE IN 6 STEPS

Get ready in 6 steps

Creation of a team dedicated to the GDPR

Mapping data processing and recommendations

Processing sheets and records of processing activities

Risk identification, analysis and assessment (PIA)

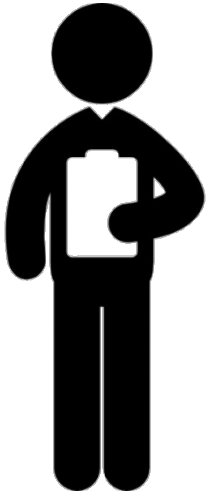
Organization of internal procedures

Document compliance

KOAN

We can help you in two ways…

INDIVIDUAL



COLLECTIVE

KOAN

V. Q&A

KOAN

Thank you

Partner

adr@koan.law

European Data Protection Officer

nha@koan.law

KOAN Law Firm

Ch. de la Hulpe 166
Terhulpsesteenweg 166
B-1170 Brussels
Belgium

+32 2 566 90 00

www.koan.law

@KoanLaw

www.linkedin.com/company/koan