General Data Protection Regulation

An interactive approach to understanding privacy

-

June 15th, 2016

Section 1: Setting the Scene

Introduction

Benny Bogaerts

Director Information Protection & Privacy Services

- *Working @ KPMG since 2001*
- *Competence Leader Information Protection & Privacy Services*

Kara Segers

Senior Expert Data Privacy & Protection

- *Working @ KPMG since 2011*
- *Data Privacy Expert in the Belgian Data Privacy Team (legal, management & technology experts*

What is Privacy, What is it Not?

What is (sensitive) Personal Data?

Family and demographic information. **Religious beliefs and race** are sensitive data

Home and work information. **Sexual orientation** is sensitive data

Fingerprints, and genetic information

Medical records. **Health information** is sensitive data

Leisure activities and hobbies. **Political opinions and group membership** are sensitive data

Online behavioral patterns, devices used, etc.

Behavioral patterns and interests

Financial information. **Union membership** is sensitive data

ETC

Travel history and location data

What is Processing?

Legislation

The General Data Protection Regulation protects "individuals with regard to the **processing** of personal data and on the free movement of such data"

Processing

Operations performed on personal data: manual or automated

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

Examples

Some examples of processing

- Remote and read only access
- Holding but not performing actions upon personal data
- Computer processing data without a human viewing it
- Use of "pseudonymized" data

KPMG

Section 2: Data Privacy Legislation

EU Privacy Directive

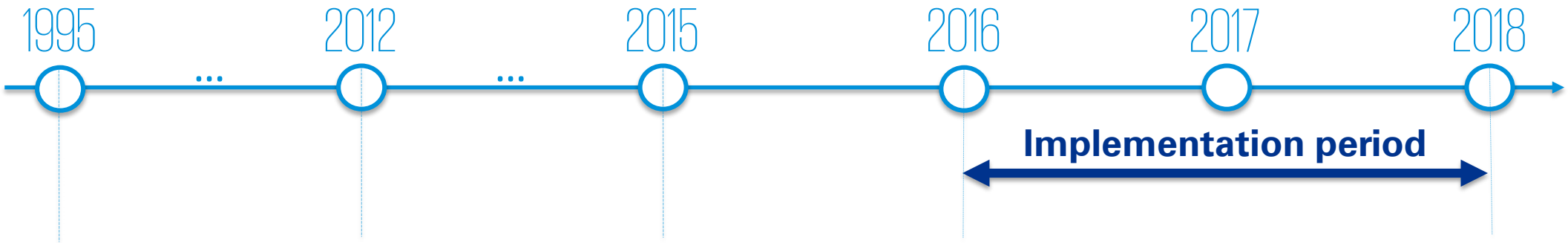
EU Directive
95-46-EC

"Our current data protection rules already contain solid data protection principles.

But they were drawn up in 1990 and adopted in 1995, when only 1% of the EU population was using the internet... and the founder of Facebook was only 11 years old!"

- Viviane Redding, European Commissioner for Justice, Fundamental Rights and Citizenship, 2010 - 2014

General Data Privacy Regulation - Timeline



EU Directive 95-46-EC

Proposal for new data privacy legislation

Agreement on the GDPR text by the European Commission, Parliament and Counsel (17/12/2015)

Publication of the General Data Protection Regulation (04/05/2016)

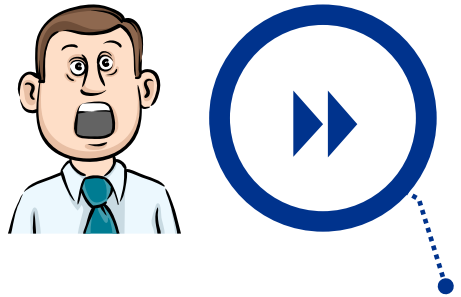
-

GDPR will enter into force (24/05/2016)

General Data Protection Regulation wll apply af of (25/05/2018)

Data Privacy Essentials

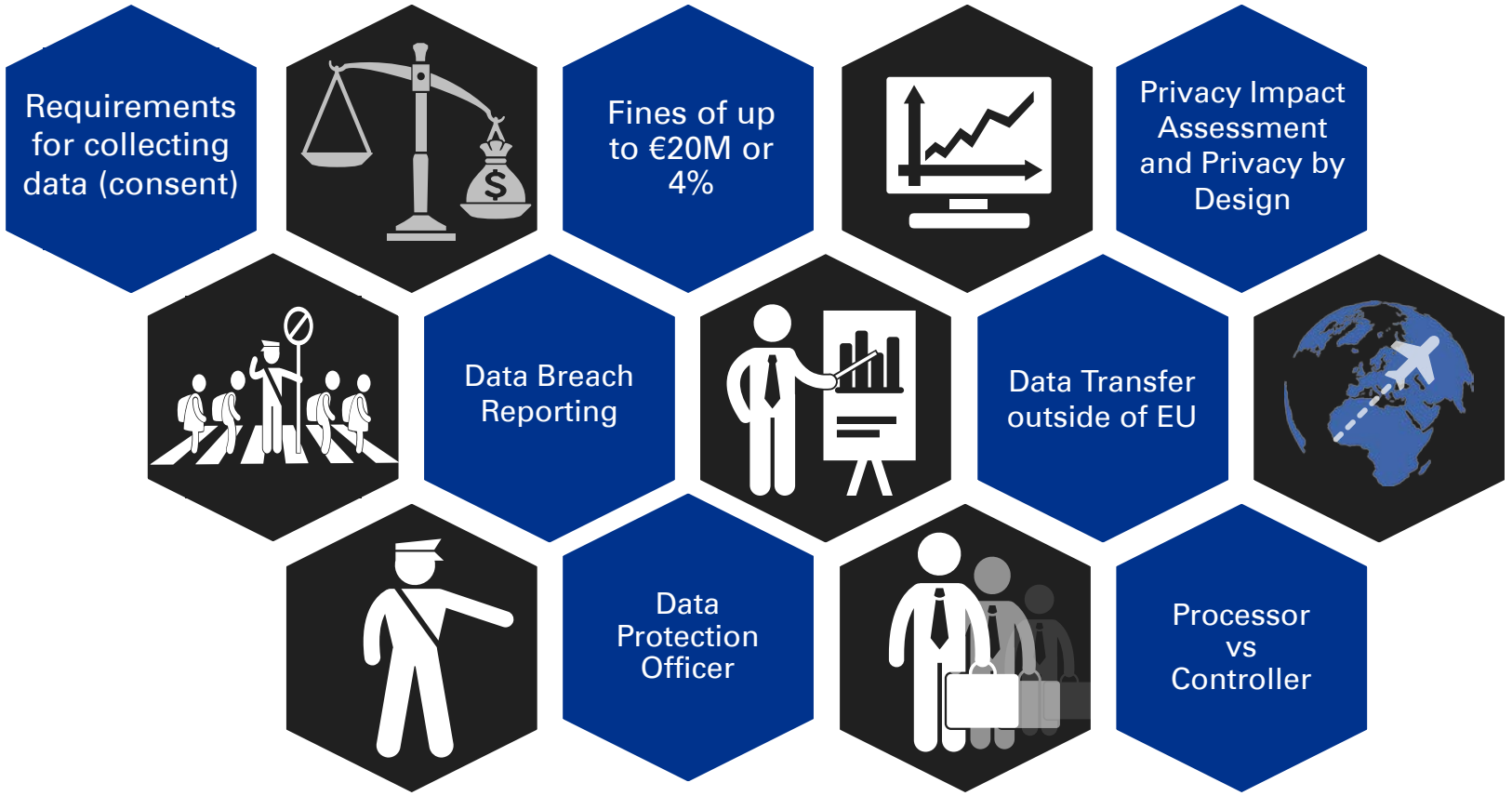
- No more national legislation, harmonization across EU
- No more mandatory notification of processing activities to the national authority (privacy commission)
- Data transfer mechanisms are clearly explained, plus there are more possibilities for data transfer.



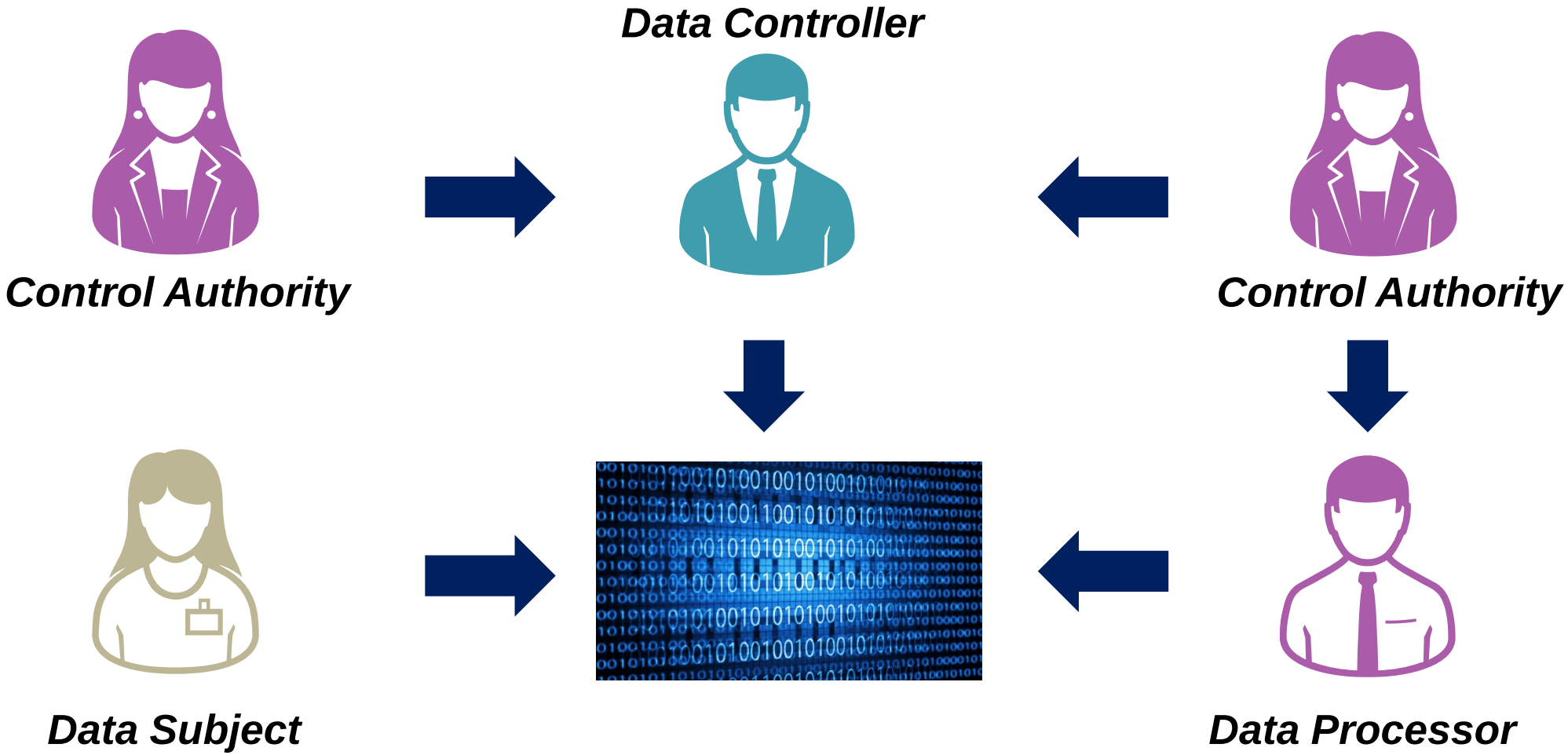
- **Increased responsibility** and accountability for controllers and processors on how they control, manage and secure their personal data.
- Mandatory **Data Privacy Officer**
- **Data Protection Impact Assessments** for new processes and systems dealing with personal data
- **Privacy by Design**, Privacy by Default
- **Increased security requirements** for personal data (e.g. encryption, anonymization)
- The **accountability** principle, demonstrating compliance (records of processing)

- **Data breach notification**
- **Consent** requirements
- Strengthened or new requirements for consent, right to be forgotten, data portability, profiling, etc.
- **High fines** in case of non-compliance

Let us take a closer look...



Controller and Processors



Data Protection Office(r)

DPO REQUIRED

- If processing is performed by a **public authority**
- where the core activities involve regular and systematic **monitoring of data subjects** on a **large scale**
- processing of **special categories of data** at large scale.

REGISTERED & SPOC

The selected DPO must be registered with the European Data Protection Supervisor, to serve as the SPOC for the organization

KNOWLEDGE

The DPO must be appointed based on his/her professional qualities: **expert knowledge** of data protection law and practices

MULTIPLE ENTITIES

The DPO may be designated for **several entities**.
Needs to be easily accessible

Position of the DPO

- DPO shall directly report to the highest level of management
- Bound by secrecy and confidentiality
- Controller/processor shall support the DPO in the execution of his/her tasks

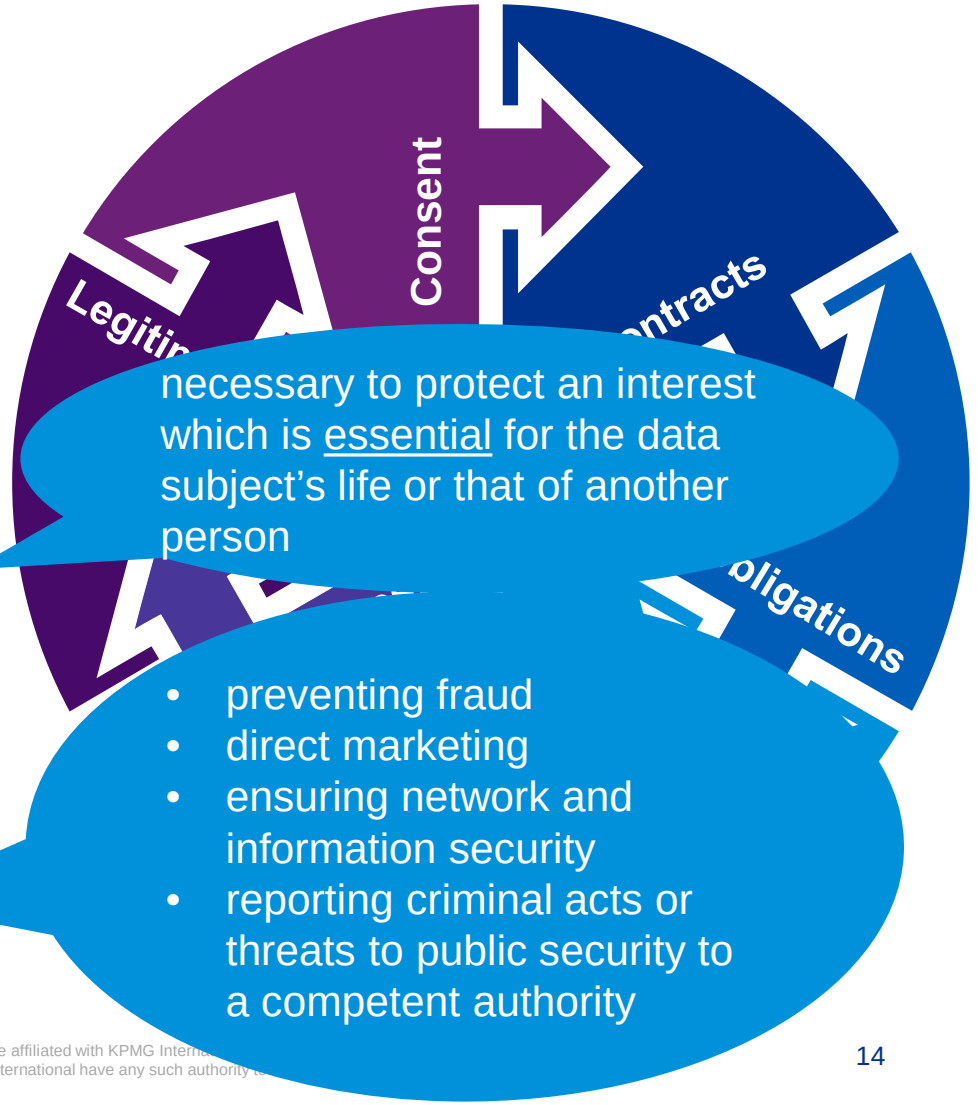
PROFESSIONAL DUTIES

A DPO may have **other professional duties**, but they must be compatible and **not result in a conflict of interest**

Consent (1/3)

Lawfulness of processing

- The data subject has given **consent** to the processing of their personal data;
- Processing is necessary for the **performance of a contract** to which the data subject is party;
- Processing is necessary for **compliance with a legal obligation** to which the controller is subject;
- Processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;
- Processing is necessary for the **performance of a task carried out in the public interest**;
- Processing is necessary for the **purposes of the legitimate interests** pursued by the controller or by a third party



Consent 2/3

Freely-Given Specific Informed

- One cannot be forced into the agreement
- Performance of the contract/ service

Provide Evidence

- Demonstrate whether consent was given

Easy Accessible Form

- Clear and plain language
- Consent for other matters than the primary purpose

Right to Withdraw

Consequences!

- Right to erasure/to be forgotten

Children's Consent

- Consent by parents under (13-16)
- reasonable efforts to verify the consent

Other

- Processing special categories of data
- Data portability

Privacy by Design / Default

Strategic

1 Privacy by Default

When?

- Always

What?

- technical and organizational measures
- only personal data is processed which are necessary for each **specific purpose**

- Such as:
  - ✓ amount of data collected
  - ✓ extent of their processing
  - ✓ period of their storage
  - ✓ accessibility

Practical

2 Privacy by Design

When?

- When determination of the **means** for processing
- When processing itself

What?

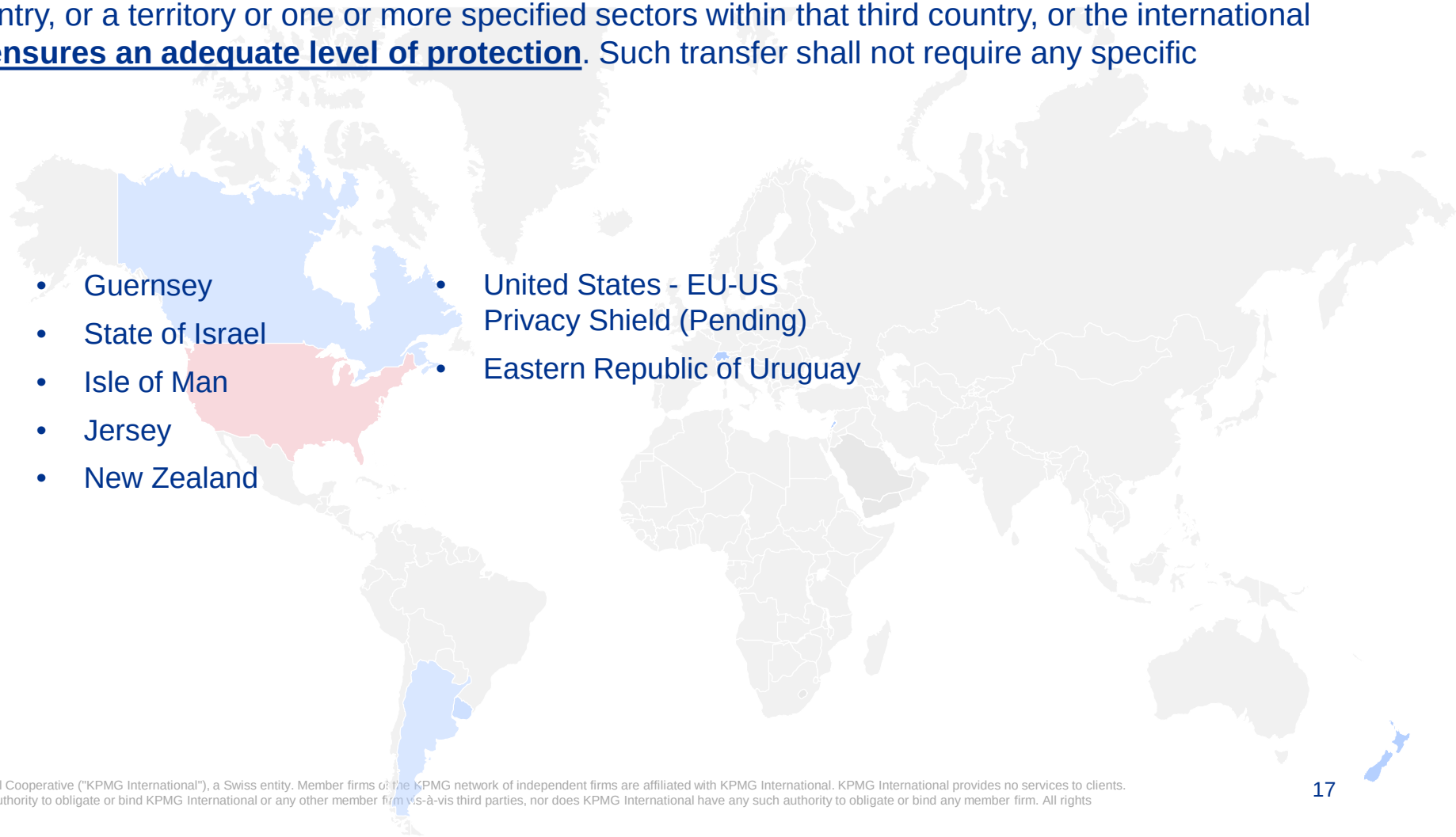
- technical and organizational measures
- implement data protection principles
- integrate the necessary safeguards (compliance + data subject rights)

Personal Data Transfers

A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, or a territory or one or more specified sectors within that third country, or the international organization in question **ensures an adequate level of protection**. Such transfer shall not require any specific authorization.

Overview:

- Andorra
- Argentina
- Canada
- Switzerland
- Faeroe Islands
- Guernsey
- State of Israel
- Isle of Man
- Jersey
- New Zealand
- United States - EU-US Privacy Shield (Pending)
- Eastern Republic of Uruguay



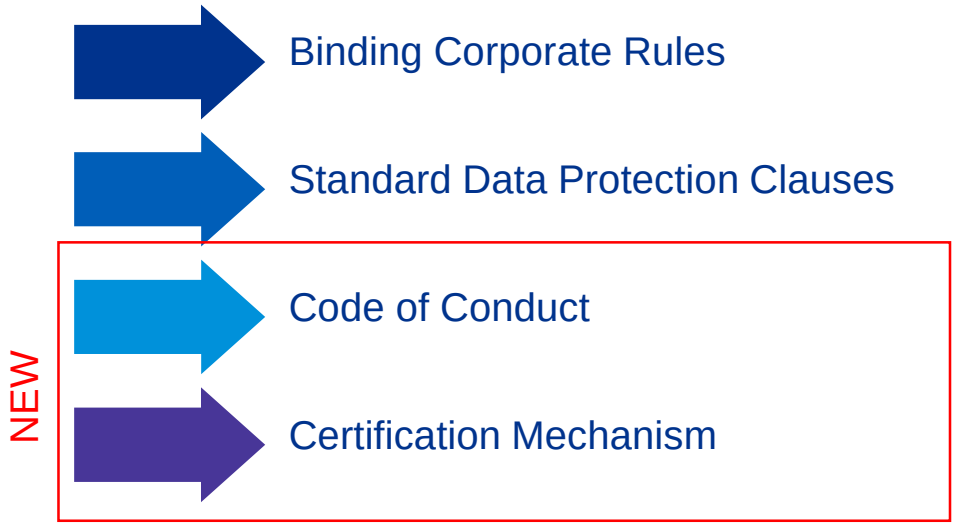
Personal Data Transfers

Transfers with an ‘Adequacy Decision’

- Andorra
- Argentina
- Canada (Commercial Organisations)
- Faeroe Islands
- Guernsey
- State of Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay

- *United States - EU-US Privacy Shield (Pending)*

Transfers by way of ‘Appropriate Safeguards’



Data Breach Reporting

Data Controller

72h

Identify → Document → Analyse → Report

Data Processor

Identify → Notify → Analyse

The 2-tiered system for penalties

If a controller or processor does not comply with the obligations of the Regulation, the supervisory authority shall impose an administrative fine up to certain thresholds, depending on Assessment Factors including the following:

Obligations with regard to consent (incl. Children's data)

Privacy by Design / Default (+ PIA)

Infringement of the processor's obligations on protecting the data

Records of processing activities (retention schedules, contact details of the processor, documentation of safeguards, etc.)

Implementing security safeguards

Personal data breaches

Data Protection Officer

Etc.

2%*

Infringement of the basic processing conditions for **consent**

Infringement of the data subject's rights: transparency, information, access, right to be forgotten,…)

Infringement of personal data transfer modalities

Non-compliance with member state laws

Non-compliance with temporary or definite suspension of processing

Etc.

4%*

Note: **% of total worldwide annual turnover of the preceding financial year.**
Source: GDPR published text, May 4th 2016

KPMG

Section 3:

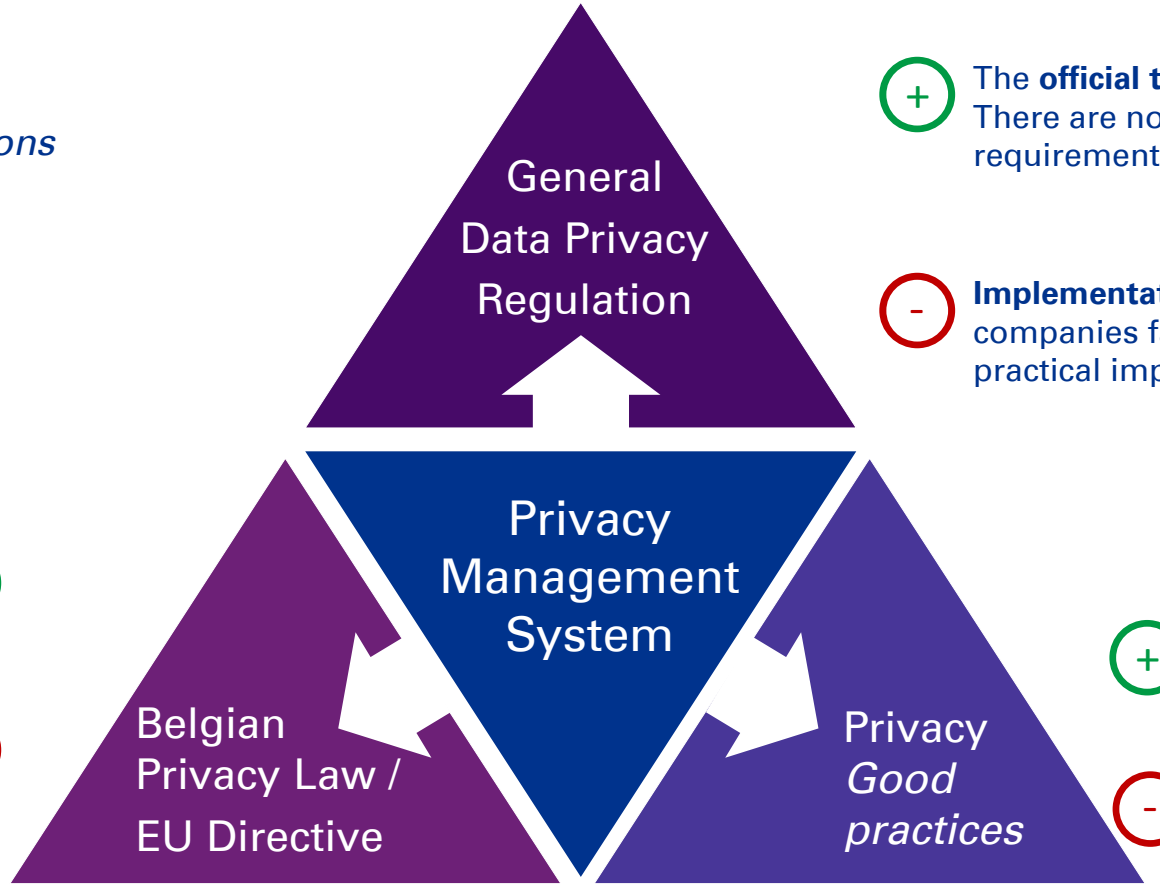
Managing the privacy environment

Approach to privacy compliance

Each of these approaches feeds into a Privacy Management Framework, which combines their strengths into one structure

There are several approaches to structuring Privacy compliance.

*Below are listed the **most commonly used within Belgium**, and pros and cons for using the approach as a basis for Privacy compliance.*



\+ The **official text** has been released in May 2016. There are no longer uncertainties on which requirements will be imposed as of 2018.

\- **Implementation guidance** is not there yet. Many companies face difficulties in understanding the practical implications.

Current **binding law** in Belgium, with well established implementation requirements. +

Directive is written for Member State implementation, not operational purposes. Both are likely to be outdated within a year. -

\+ Globally accepted good practices developed for **business use,** which underlie EU privacy laws

\- Not legally binding

Approach to privacy compliance - Privacy Management Framework

PRIVACY PRINCIPLES

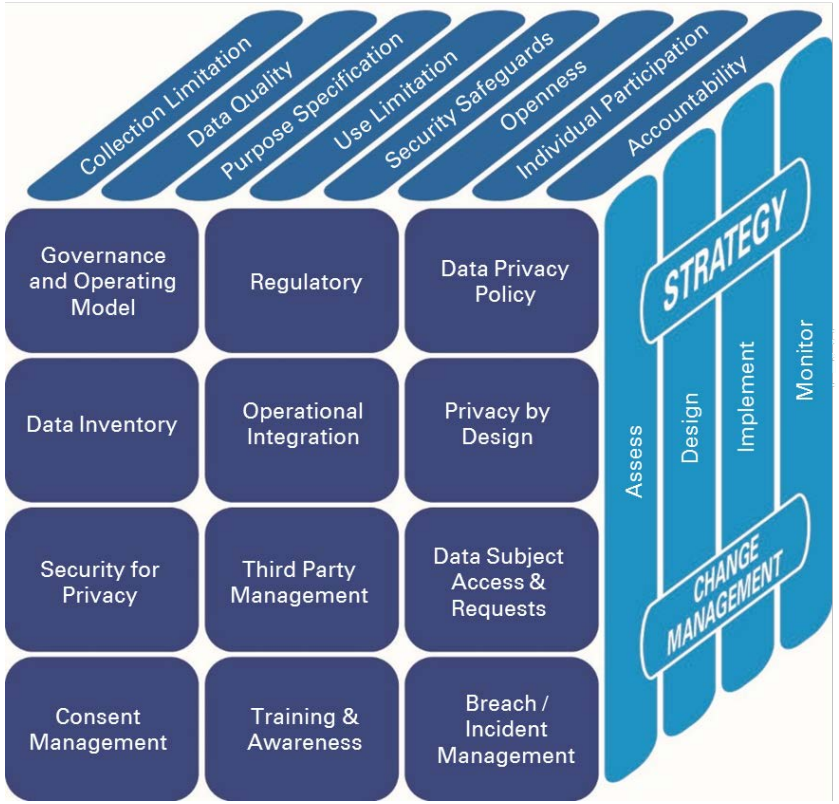
Privacy elements are viewed against the OECD Privacy Principles, which provide the foundation for the EU Directive, General Data Privacy Regulation and our Privacy Management Framework

PRIVACY MANAGEMENT FRAMEWORK

Our framework elements are the distinct elements that organisations employ to mange Privacy. They provide a practical and pragmatic structure for organising the day-to-day management and oversight required to manage Privacy.

KPMG APPROACH

Our Privacy Service has been designed on the basis that organisations need tailored risk based solutions to address their individual Privacy needs, risk appetite and future business strategy. Its modular and layered structure enables targeted and tailored solutions to be designed, developed, implemented and monitored consistently, cutting through the complexity of Privacy and complex global organisations.



Privacy Controls - examples

GOVERNANCE

- Privacy Management System
- Defined qualifications of internal personnel w.r.t. data privacy
- Demonstrate compliance by certifications, seals, accreditations, code of conducts, etc.

REGULATORY

- Framework for (personal) data transfer mechanisms
- Obtain legal opinions regarding recent developments in law

PRIVACY POLICY

- Data privacy policy is clear and conspicuous
- Data privacy policy and procedures are periodically reviewed

SECURITY

- Integrate data privacy into an information security policy
- Data-loss prevention strategy
- Procedures for physical access

THIRD PARTY

- Third-party due diligence for data privacy
- Systems and procedures for disclosure of personal information to third-parties

DATA SUBJECT ACCESS

- Procedures to respond to requests for information
- Accounting of disclosures

CONSENT

- Data privacy notice is clear and conspicuous
- Procedures and policies for obtaining valid consent

TRAINING & AWARENESS

- Specific privacy training reflecting job content
- Mandatory attendance to privacy awareness training

PRIVACY BREACH

- Data Breach response plan
- Data Breach notification by the processor

INVENTORY

- Classification framework for personal data
- Ownership for keeping the data inventory up-to-date has been formally assigned

INTEGRATION

- Policies and procedures for collection and use of sensitive personal data
- Policies and procedures for de-identification of personal data
- Policies and procedures for the minimization of personal data

PRIVACY BY DESIGN

- Conduct a DPIA for new programs, systems, processes
- Review of processing activities in compliance with the DPIA

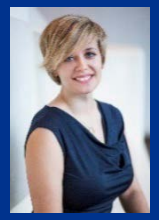
Questions? Yes, please!

Thank you

Contact us

Benny Bogaerts
Director Information Protection Services

M: +32 477 30 14 49
E: bbogaerts@kpmg.com



Kara Segers
Senior Advisor Data Privacy & Protection

M: +32 494 49 02 16
E: ksegers@kpmg.com

DRIVEN BY BUSINESS

We work with our clients to move their business forward. Positively managing cyber risk not only helps take control of uncertainty across business; it can be turned into a genuine strategic advantage.

RAZOR SHARP INSIGHTS

In a fast-moving digital world of constantly evolving threats and opportunities, you need both agility and assurance.

Our people are experts in both cyber security and our priority sectors, which means we give our clients leading edge insight, ideas and proven solutions to act with confidence.

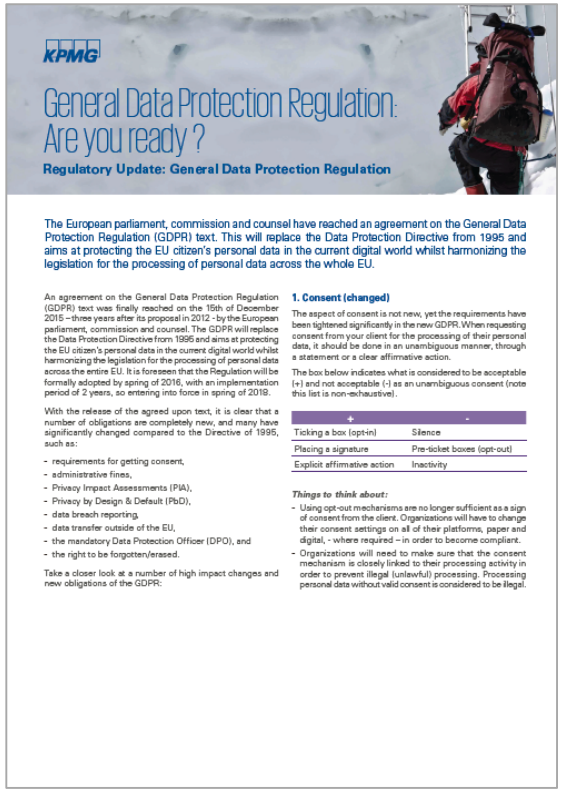
SHOULDER TO SHOULDER

We work with our clients as long term partners, giving them advice and challenge to make decisions with confidence. We understand that this area is often clouded by feelings of doubt and vulnerability so we work hand-in-hand with them to turn that into a real sense of security and opportunity.

KPMG

Appendix

KPMG Publications



KPMG

General Data Protection Regulation: Are you ready ?

Regulatory Update: General Data Protection Regulation

The European parliament, commission and counsel have reached an agreement on the General Data Protection Regulation (GDPR) text. This will replace the Data Protection Directive from 1995 and aims at protecting the EU citizen's personal data in the current digital world whilst harmonizing the legislation for the processing of personal data across the whole EU.

An agreement on the General Data Protection Regulation (GDPR) text was finally reached on the 15th of December 2015 – three years after its proposal in 2012 - by the European parliament, commission and counsel. The GDPR will replace the Data Protection Directive from 1995 and aims at protecting the EU citizen's personal data in the current digital world whilst harmonizing the legislation for the processing of personal data across the entire EU. It is foreseen that the Regulation will be formally adopted by spring of 2016, with an implementation period of 2 years, so entering into force in spring of 2018.

With the release of the agreed upon text, it is clear that a number of obligations are completely new, and many have significantly changed compared to the Directive of 1995, such as:

- requirements for getting consent,
- administrative fines,
- Privacy Impact Assessments (PIA),
- Privacy by Design & Default (PbD),
- data breach reporting,
- data transfer outside of the EU,
- the mandatory Data Protection Officer (DPO), and
- the right to be forgotten/erased.

Take a closer look at a number of high impact changes and new obligations of the GDPR:

1. Consent (changed)

The aspect of consent is not new, yet the requirements have been tightened significantly in the new GDPR. When requesting consent from your client for the processing of their personal data, it should be done in an unambiguous manner, through a statement or a clear affirmative action.

The box below indicates what is considered to be acceptable (+) and not acceptable (-) as an unambiguous consent (note this list is non-exhaustive).

+	-
Ticking a box (opt-in)	Silence
Placing a signature	Pre-ticket boxes (opt-out)
Explicit affirmative action	Inactivity

Things to think about:

- Using opt-out mechanisms are no longer sufficient as a sign of consent from the client. Organizations will have to change their consent settings on all of their platforms, paper and digital, - where required – in order to become compliant.
- Organizations will need to make sure that the consent mechanism is closely linked to their processing activity in order to prevent illegal (unlawful) processing. Processing personal data without valid consent is considered to be illegal.