ALLEN & OVERY

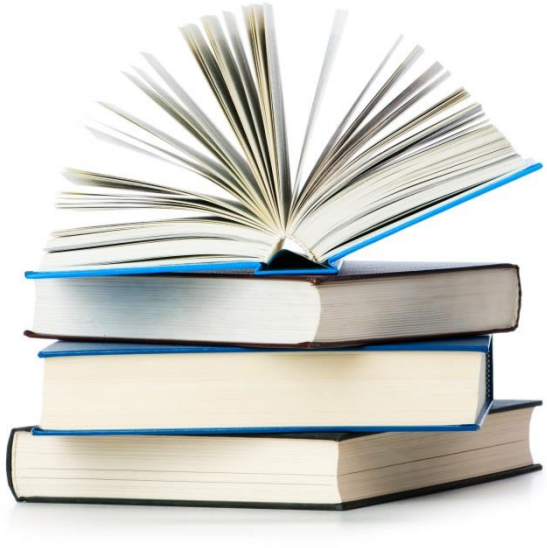
The ABC of GDPR

Kaat Van Delm

01 March 2018

Agenda

1. An introduction to GDPR
2. GDPR: Core principles
3. Specific points of attention for marketing
4. To do's



An introduction to GDPR

What is 'GDPR'?

= legislation determining in which situations and under which conditions **personal data** can be **Processed**

01 General Data Protection Regulation

02 Not new!

03 Regulation: rules apply throughout the whole EU

04 Fundamental principles do not change however become more severe

05 D-Day: 25 May 2018

So… (only) 85 days left

The GDPR will apply from 25 May 2018

National complementing legislation is still to be published in many Member States

Many clients **tracking industry association guidance** and **competitor approaches**

Member States have certain areas in which they **can derogate**

National regulator guidance and tools are appearing weekly

BR:14135331.1

GDPR: essential terminology

Personal data

All information concerning an identified or identifiable natural person (the 'data subject')

Eg. adress, telephone number, location data, photos, camera images, identification number electronic device, combination of elements characterising a person

Processing

Use of personal data, whether performed through automated means or not

Eg. Collecting, structuring, saving, changing, consulting, using, spreading, deleting etc.

GDPR: essential terminology (cont'd)

Controller — who determines the purpose and means of the processing

- Legal criterion, cannot be altered contractually
- Controller mostly responsible for legal compliance

Processor — who processes personal data **on** behalf of the controller

- Only allowed to process on basis of written instructions (unless if a legal obligation exists)
- Co-responsibility?

GDPR: essential terminology (cont'd)

Sensitive personal data

personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural peron, data concerning health or data concerning a natural person's seks life or sexual orientation

- In principle prohibited
- Some limited exceptions to the prohibition exist
  Eg. Explicit consent

Expanded territorial reach

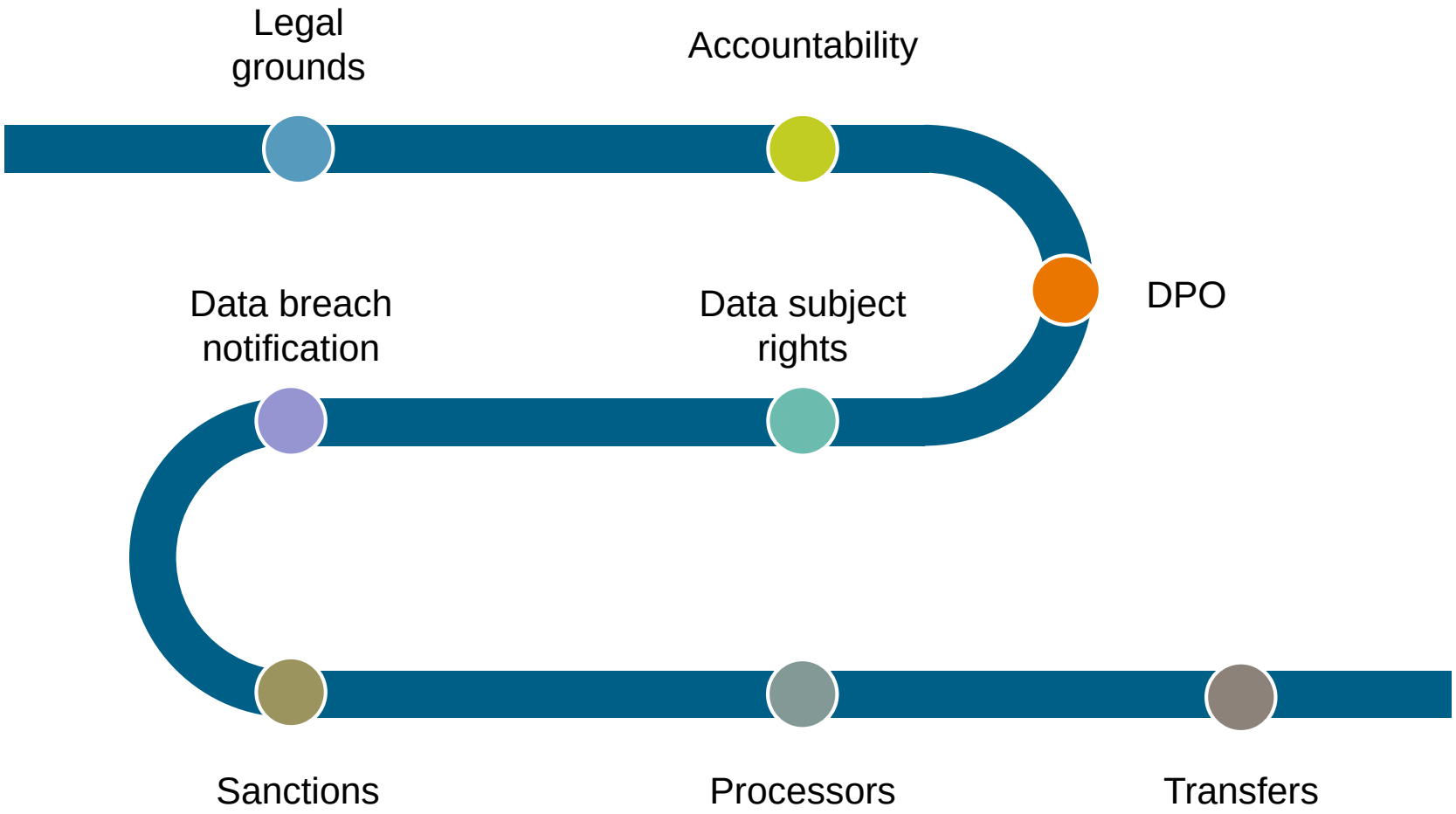
The GDPR catches data controllers and processors established *outside* the EU where their processing activities relate to:

– The activities of a **EU entity**

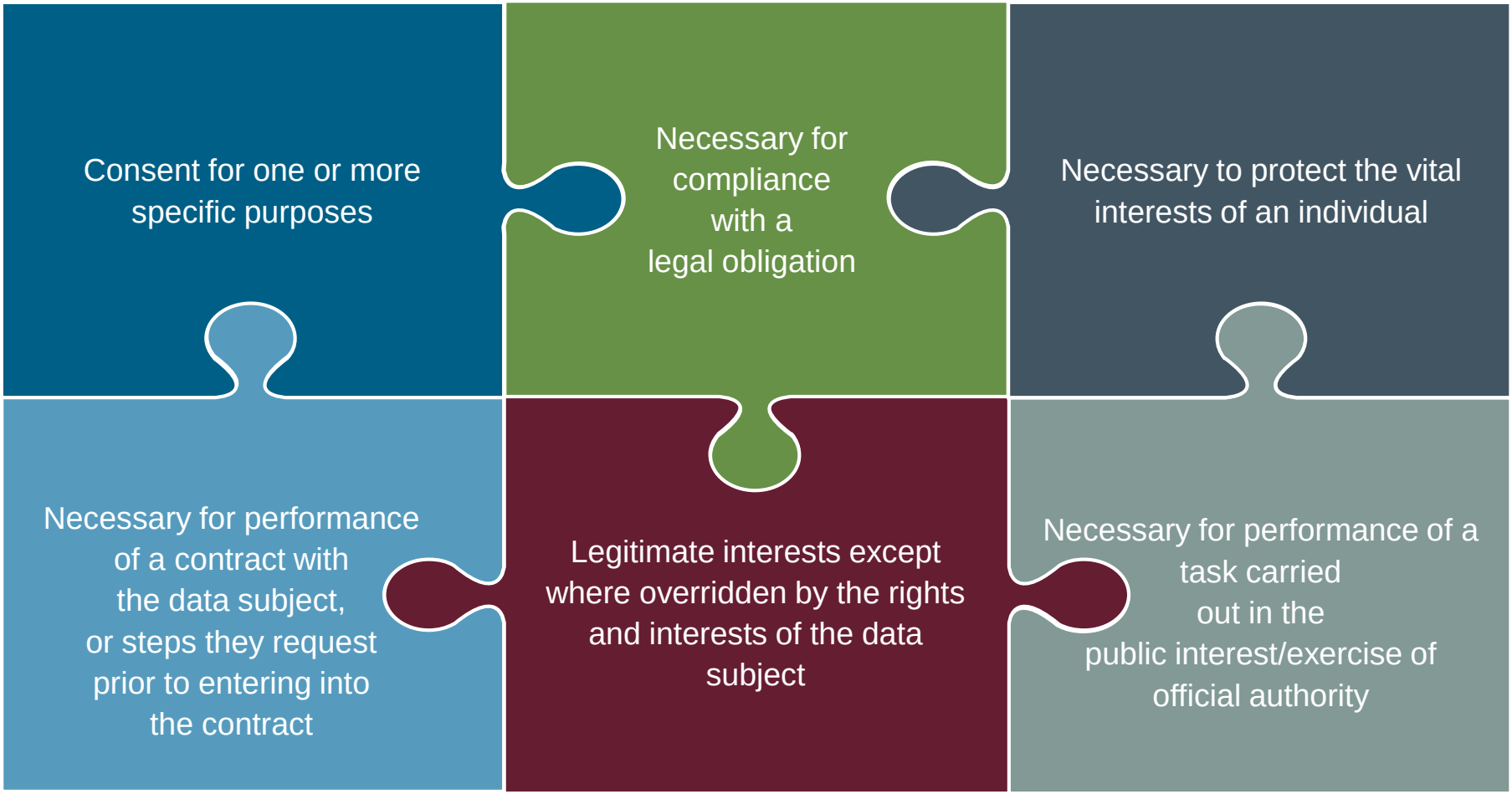
– Offering **products and services** (even if for free) to EU citizens

– **Monitoring** the behaviour of EU citizens

GDPR: Core principles



Legal grounds



Legal grounds – Consent is increasingly difficult

Consent

- Data controllers are required to **demonstrate** that consent was **freely given, specific, informed and unambiguous**
- When assessing whether consent is freely given, “utmost account” shall be taken of whether provision of a service/performance of a contract is made conditional on consent
- Must be **clearly distinguished** from other matters, **intelligible, accessible and in clear and plain language**
- Must be as easy to give as to **withdraw consent**
- **Parental consent** is required where information society services are offered to children below the age of 16 (Member States can lower the age threshold to 13, which the UK plans to do).
- Must take reasonable steps to verify
- **No reliance** on silence or pre-ticked boxes

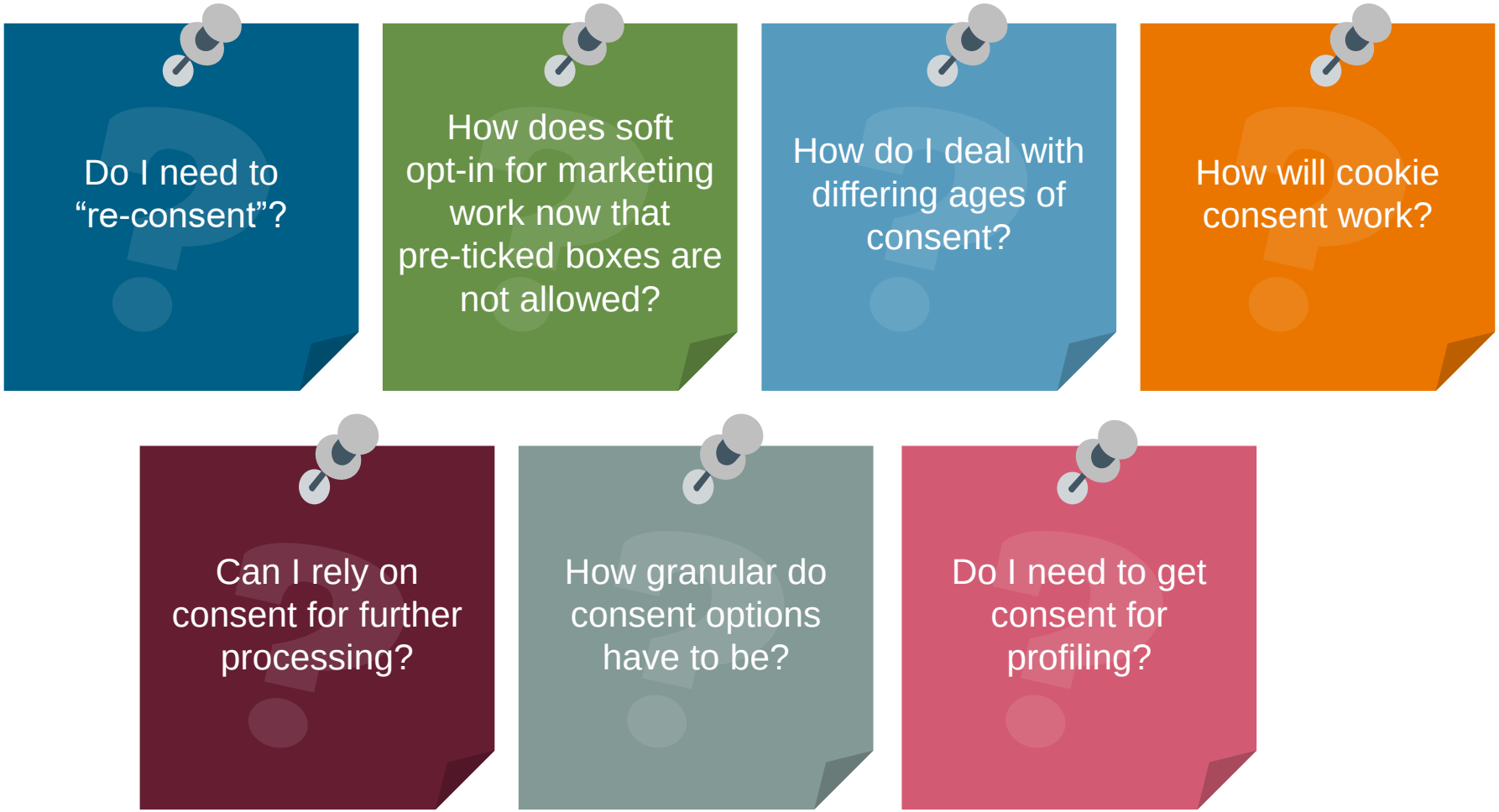
Legal grounds – summary

Legal basis – most relevant ones
– Consent
– Performance of a contract
– Legitimate interests
– Legal obligation

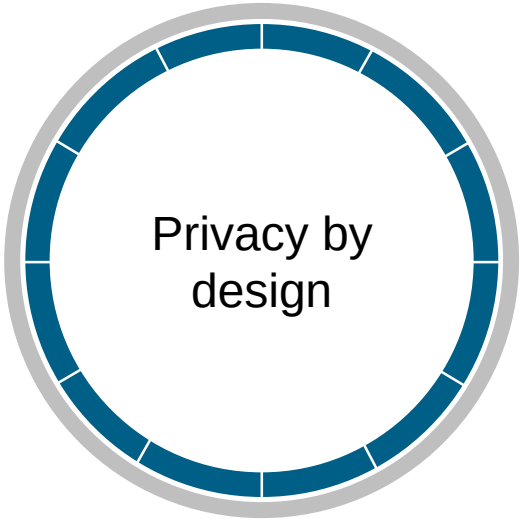
Consent needs to be given through an **affirmative action**

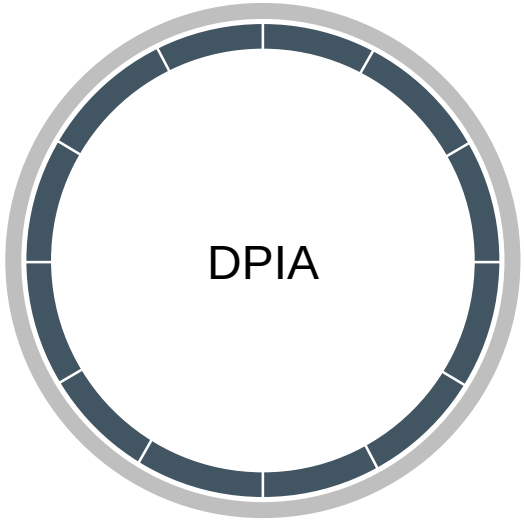
Consent can at any time be **withdrawn**

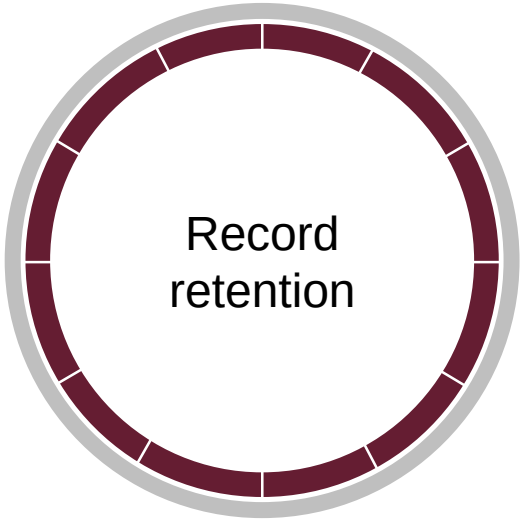
You might also ask…



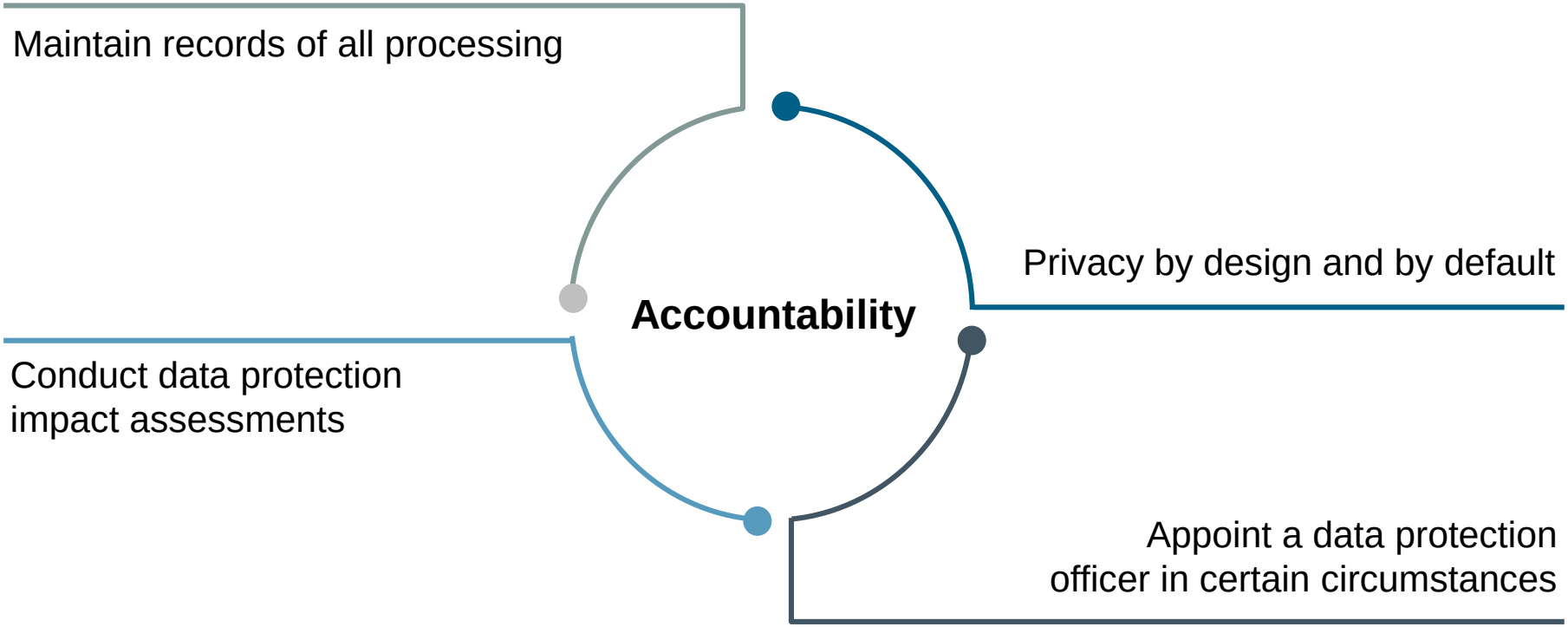
Accountability







Accountability – GDPR requires controllers to demonstrate compliance



Accountability – Privacy by design/default

1. By design

Implement appropriate technical and organisational measures

- To comply with the GDPR requirements
- To protect the rights of data subjects

2. By default

Implement appropriate technical and organisational measures

- To ensure that, by default, only personal data which are necessary for each specific purpose of processing are processed

Data Protection Officer (DPO)

Does your company need one?

YES if

- You are a public authority or body
- Your core activities consist of processing which by its nature, scope or purposes requires regular and systematic monitoring of data subjects on a large scale
- Your core activities involve large scale processing of special categories of personal data and data relating to criminal convictions and offences

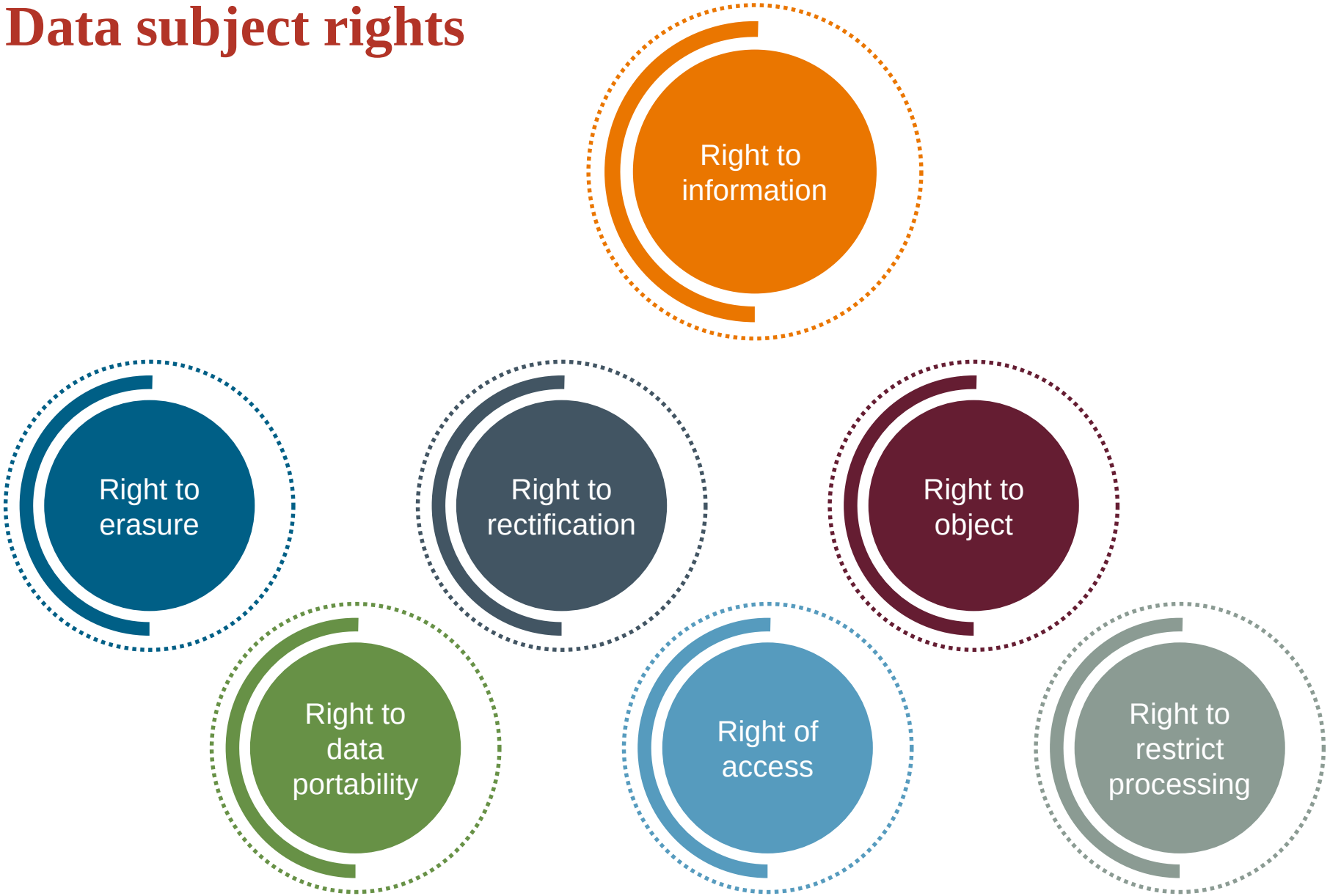
Who should it be?

- Expert knowledge, no conflict, reporting directly to highest management levels, various specified tasks, protected

Article 29 Working Party guidance

- If appointed voluntarily (or given that title) they will be subject to the same requirements

Data subject rights



Data subject rights – Right to be forgotten and data portability

In certain circumstances, individuals can require the erasure of their personal data

Exceptions apply

In certain circumstances, individuals can request the portability of their personal data

Exceptions apply

Data breach notification

Data controllers must notify data breaches to the DPA without undue delay and where, feasible, within **72 hours** of awareness. A "***reasoned justification***" must be provided if this timeframe cannot be met.

An **exception** to the notification requirement is where the breach is unlikely to result in a risk for the rights and freedoms of individuals.

Sanctions

When deciding whether to impose a fine, DPAs will take into account:

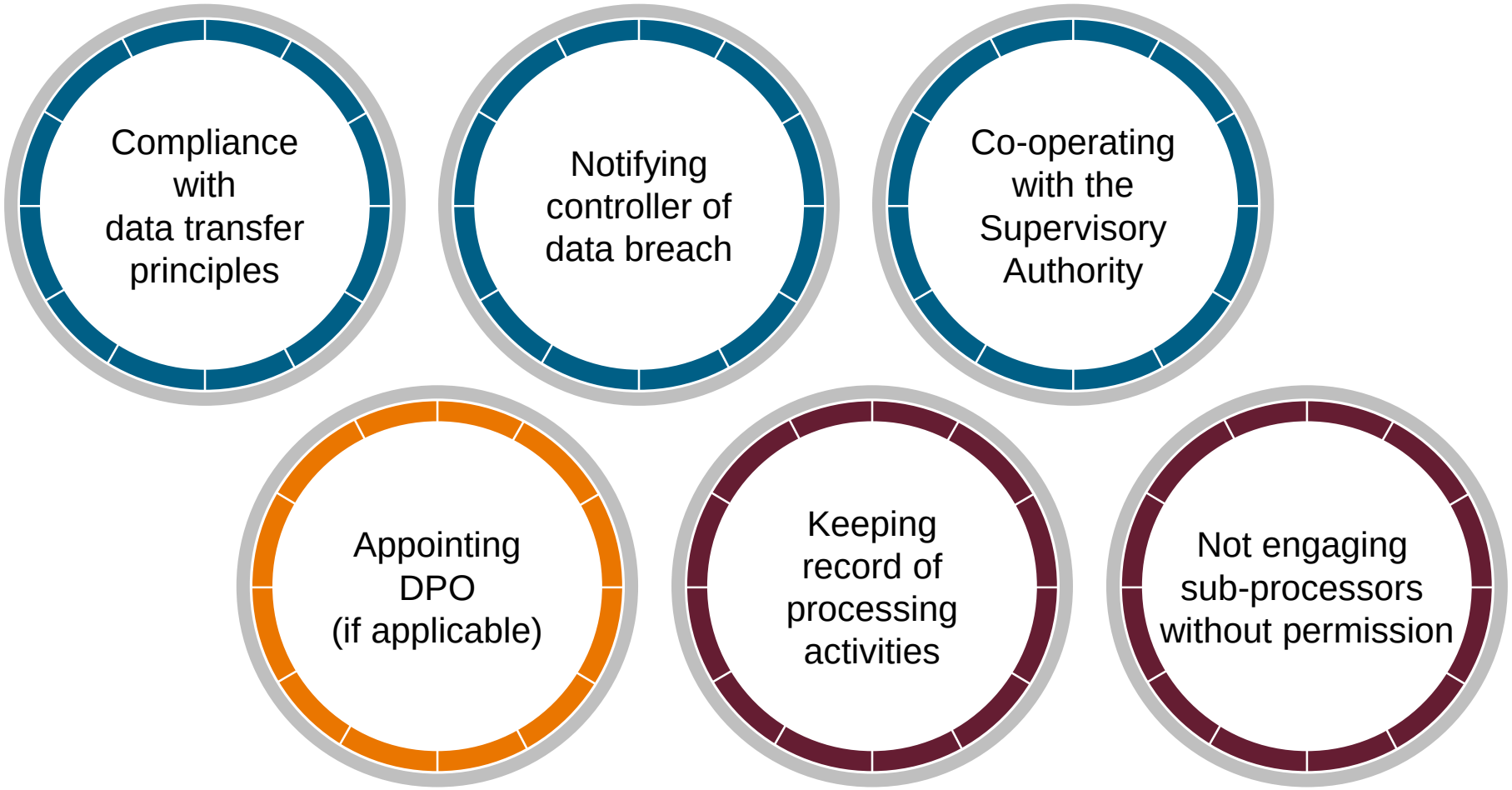
– The nature, gravity and duration of the infringement

– The purpose of the processing concerned

– The number of data subjects affected and the level of damage suffered by them

Fines of up to 2 – 4 % of annual worldwide turnover

Processors – some direct obligations, such as…



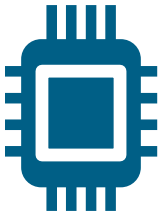
Processors

A controller must

Only use processors who provide sufficient guarantees to implement appropriate technical and organisational measures so that

- Processing meets the requirements of the GDPR; and
- The protection of the rights of data subjects is ensured

Give written authorisation (general or specific) for any sub-processing



Put in place a binding contract setting out:

- Subject matter, duration, nature and purpose of the processing
- Obligation only to process the personal data in accordance with documented instructions from the controller
- Assistance to be provided to the controller (in various areas)
- Obligation to have appropriate technical and organisational measures in place to assist with data subjects rights
- Provision of certain information
- Those who will process must commit to appropriate confidentiality obligations

Transfers – data streams outside EEA

Within EEA

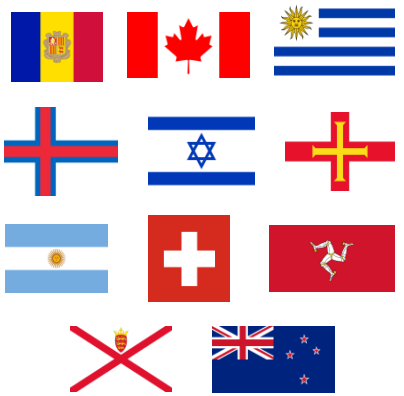
In principle permitted

From EEA to non-EEA

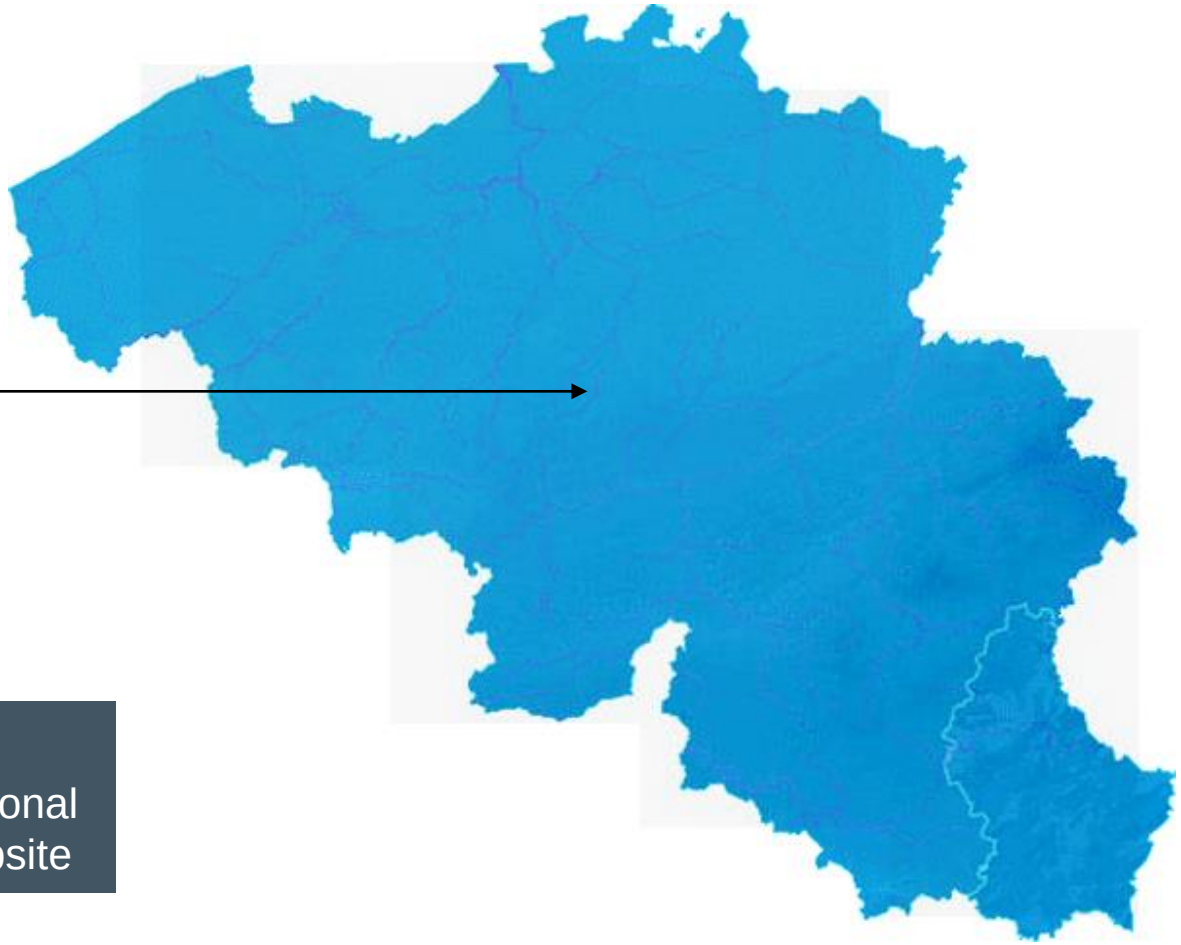
Countries **without** an adequate level of protection

- Contractual arrangements
  - Model contract clauses
  - Binding corporate rules
- Performance of a contract
- Consent

Countries **with** an adequate level of protection



A day in the life of a consumer



Mr John Smith

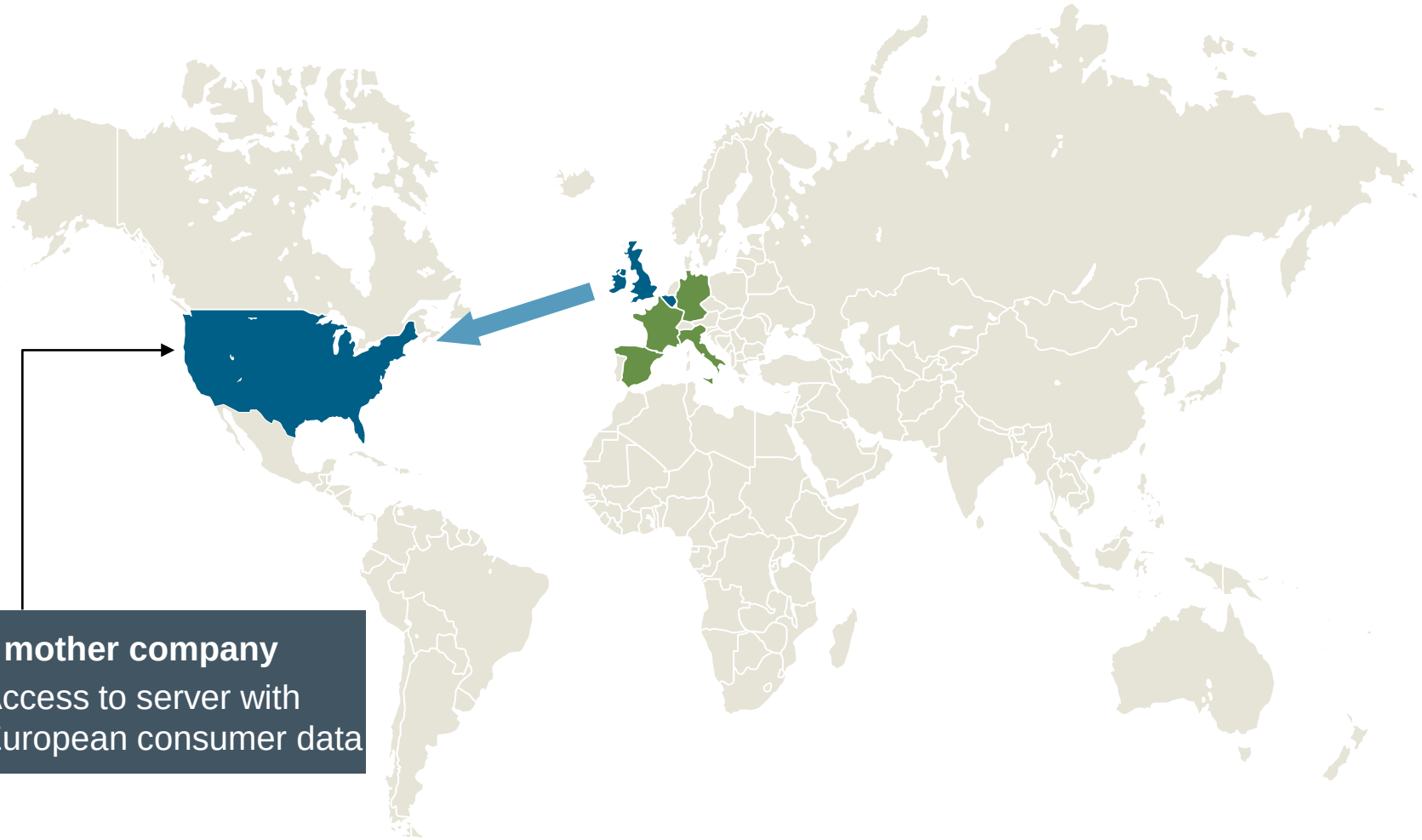
A Belgian consumer whose personal data are captured through a website

A day in the life of an expat

European headquarters

Server with all European consumer data in UK

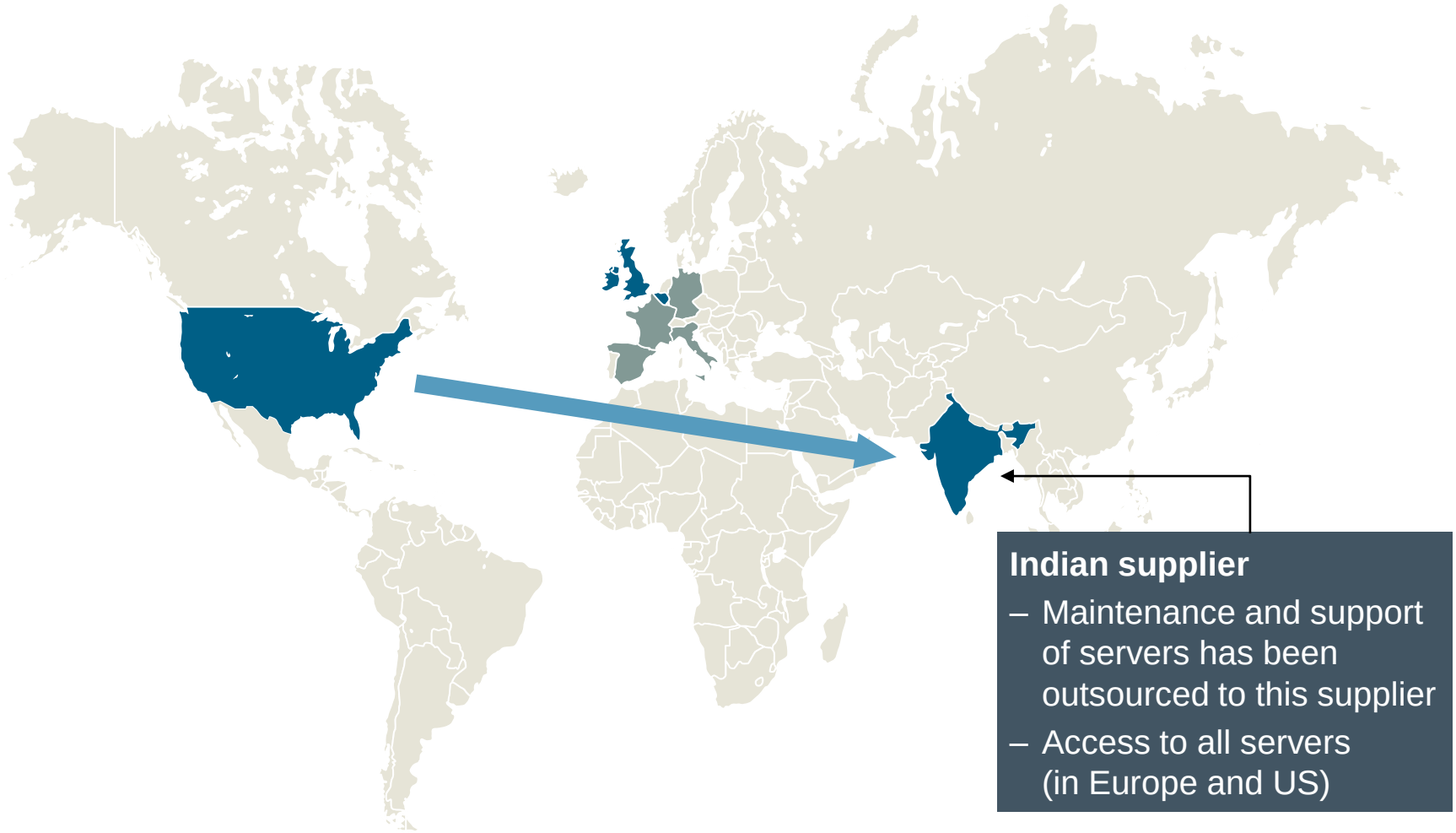
A day in the life of an expat (cont'd)



US mother company

– Access to server with European consumer data

A day in the life of an expat (cont'd)



Indian supplier

- Maintenance and support of servers has been outsourced to this supplier
- Access to all servers (in Europe and US)

Specific points of attention for marketing

Privacy notices: must be comprehensive, specific and dynamic

Transparency

The level of detail to be provided to data subjects has increased

- Identity and contact details of the controller and DPO
- Purpose and legal basis for processing each category of data
- Where legitimate interest are the legal basis for processing, what it is
- Recipient or categories of recipients
- Transfers outside the EEA and safeguards in place
- Retention period for each category of data
- Existence of each of the data subject's rights
- Right of complaint
- Any secondary purposes for processing

Privacy notices

Transparency

What does a privacy notice look like?

- A privacy notice does not necessarily have to be housed in a single document
- Information can be channelled through more than one source:
  - Orally (eg onboarding, training)
  - Documents (eg policies, employment contracts, settlement agreements)
  - Website
  - Mobile apps
  - A combination of sources

Automated decisions – without human involvement

Individuals have the **right not to be subject to** decisions based solely on automated processing (including profiling) which produces legal effects concerning them or which similarly significantly affects them

Exceptions include where:

– The individual has given **explicit consent;**

– Making the decision is authorised by EU or Member State law and which sets out safeguards; or

– It is necessary for entry into or **performance of a contract** with the data subject

Notification obligations to individuals – information about the logic and significance

Can be made with or without profiling

More restrictive where special categories of data processed

Children and 'information society services'

Information society services

Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of the service recipient

Parental consent required until the age of 16 years

Member states may lower the age to 13 years

Heated debate: consent for direct marketing purposes in Belgium?

Legal basis for direct marketing in Belgium?

Lobby: legitimate interest, balanced

GDPR: legitimate interest is possible, if not consent

National legislation: Belgian Code of Economic law requires, regarding electronic direct marketing, **active consent**, limited exceptions apply (eg.existing customer of similar services)

To do's

How to prepare?

1. Evaluate your processing activities

- Check contracts (suppliers, customers, data subjects, employees, processors)
- Map internal personal data streams (in a register)
- Map international personal data streams? (Legal basis available?)

How to prepare? (cont'd)

2. Evaluate communication with data subjects

- Analyse legal basis: Consent or balancing exercise legitimate interest?
- Consent: comply with conditions
- Balancing exercise: express legitimate interest for processing to data subject
- Information: displayed in clear and plain language?
- Requirement assigning DPO?

How to prepare? (cont'd)

3. Policies and procedures

- Procedures: international data streams, data breaches, retention
- Training marketing team: change of culture
- Know and respect rights of data subjects

Questions?

Peter Van Dyck

Peter.VanDyck@allenovery.com

Filip Van Elsen

Filip.VanElsen@allenovery.com

These are presentation slides only. The information within these slides does not constitute definitive advice and should not be used as the basis for giving definitive advice without checking the primary sources.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.