KPMG Law

Countdown to compliance: Preparing for the EU Data Act

Laura Vanuytrecht & Raf Schoefs

4 September 2025

Presenters

Raf Schoefs

Senior Counsel
Technology, IP & Data

E-mail: rschoefs@kpmglaw.be
Tel: +32 475 42 93 36

Laura Vanuytrecht

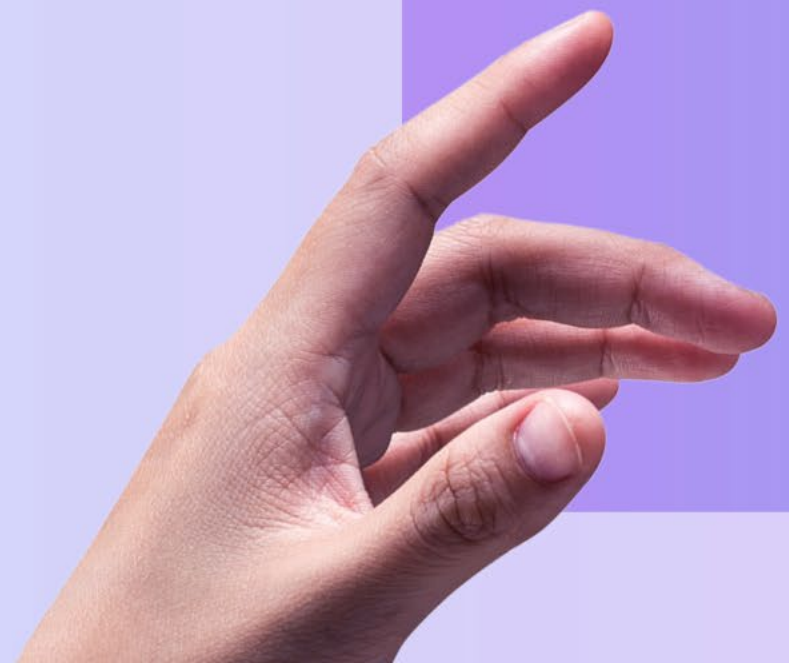
Counsel
Technology, IP & Data

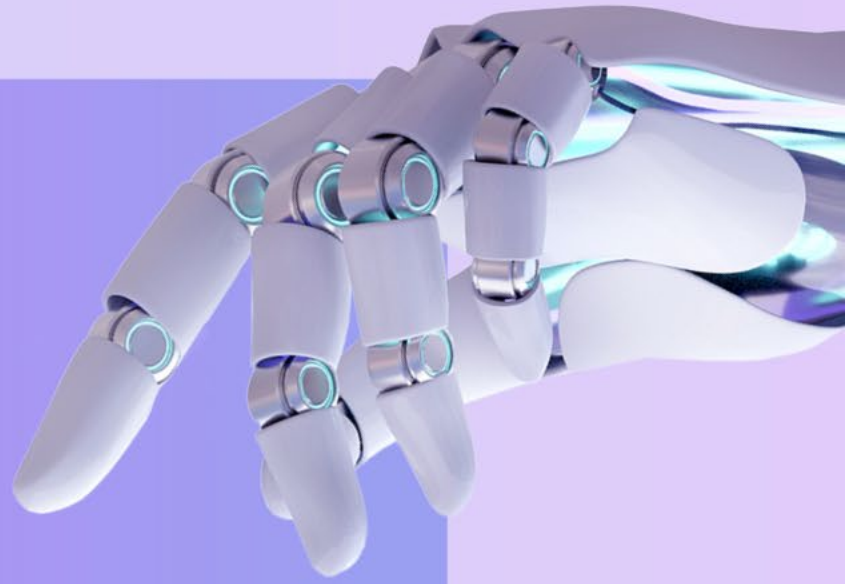
E-mail: lvanuytrecht@kpmglaw.be
Tel: +32 498 24 11 35

Contents

01

Introduction





1. Introduction

EU Data Act

A Regulation on fair access to and use of data

Background

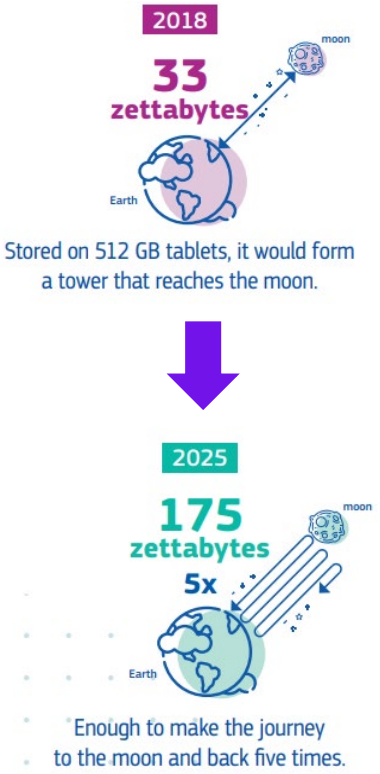
- Cornerstone of the European Strategy for Data
- Data is everywhere
  - Increasing amount of (industrial) data, but who controls?
  - Increasing dependency on data processing services, but vendor lock-in risks

Key objectives of the Data Act

- Fostering a competitive and fair data market, with a focus on industrial data
- Facilitating switching between data processing services
- Removing technical and legal barriers to data mobility

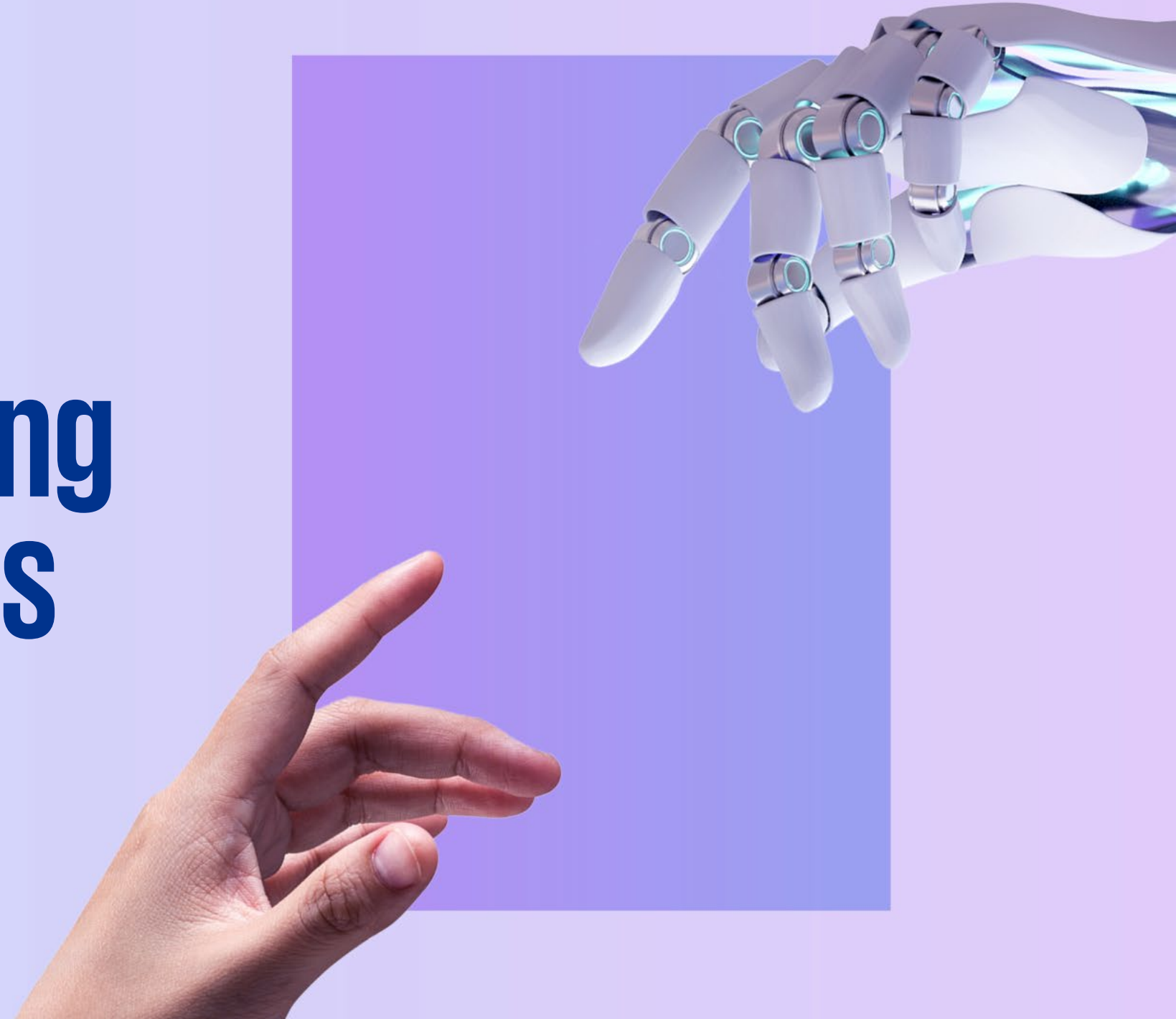
The Data Act in practice

- Directly applicable rules across the entire EU
- Horizontal rules that apply across all sectors



02

Data sharing and access

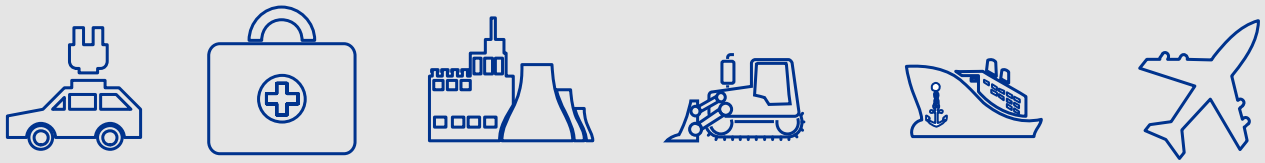


2.1. Scope: Which IoT products and services are covered?

The Data Act gives users the right to access and share data generated by connected products and related services

Connected Product

- **an item that obtains, generates or collects data concerning its use or environment**, and
- **that is able to communicate product data** via an electronic communications service, physical connection or on-device access, and
- whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user.



Related Service

- **a digital service**, other than an electronic communications service, including software, **which is connected with the product** at the time of the purchase, rent or lease **in such a way that its absence would prevent the connected product from performing one or more of its functions**,
- or which is subsequently connected to the product by the manufacturer or a third party to add to, **update or adapt the functions of the connected product**.

2.1. Scope: Which IoT data is covered?

Product Data

Data obtained, generated or collected by a connected product and which relates to its use, performance or environment

Related Service Data

Data representing user action, inaction and events related to the connected product during the provision of a related service

Metadata

A structured description of the contents or the use of data facilitating the discovery of that data

Readily available data

Product data / Related service data that can lawfully be obtained, without disproportionate effort going beyond a simple operation

What is covered?

- **Raw and pre-processed data** (or source or primary data) which:
  - is not substantially modified
  - is generated without any further form of processing
  - has been pre-processed for the purpose of making them understandable and usable
- **Personal and non-personal data**
  - Without prejudice to the GDPR
- **Trade secrets**
  - But safeguards

What is not covered?

- **Highly enriched data** (or inferred or derived data) which results from additional investments (e.g. by way of proprietary, complex algorithms)
- **Content**
  - e.g. textual, audio or audiovisual content

2.1. Scope: Which IoT data is covered?

Example: Connected car

Product data

- Speed
- Fuel level
- Engine temperature
- Tire pressure
- Braking patterns

Related service data

- Route history
- Live traffic updates
- Music preferences
- Driver profiles

Metadata

- Timestamp & location (when/where engine data was recorded)
- Sensor ID / software version (which component produced the data)
- Transmission details (network type, data size, upload time)
- User/session info (which driver profile or mode was active)

Highly enriched data

- Driver risk/behavior scores (e.g. “aggressive driver”)
- Insurance risk profiles (crash likelihood)
- Predictive maintenance forecasts (engine failure in 3,000 km)
- Smart route efficiency ratings (combining traffic, weather, consumption)

2.1. Scope: Who are the key actors?

01

Users

- a natural or legal person that owns a connected product or to whom temporary **rights to use** that connected product have been contractually transferred, or that receives related services

02

Data holder

- a natural or legal person that has the **right or obligation to use and make available data**

Exceptions

- Micro & small enterprises
- Medium-sized enterprises

03

Data recipient

- **a natural or legal person**, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product/related service, **to whom the data holder makes data available**

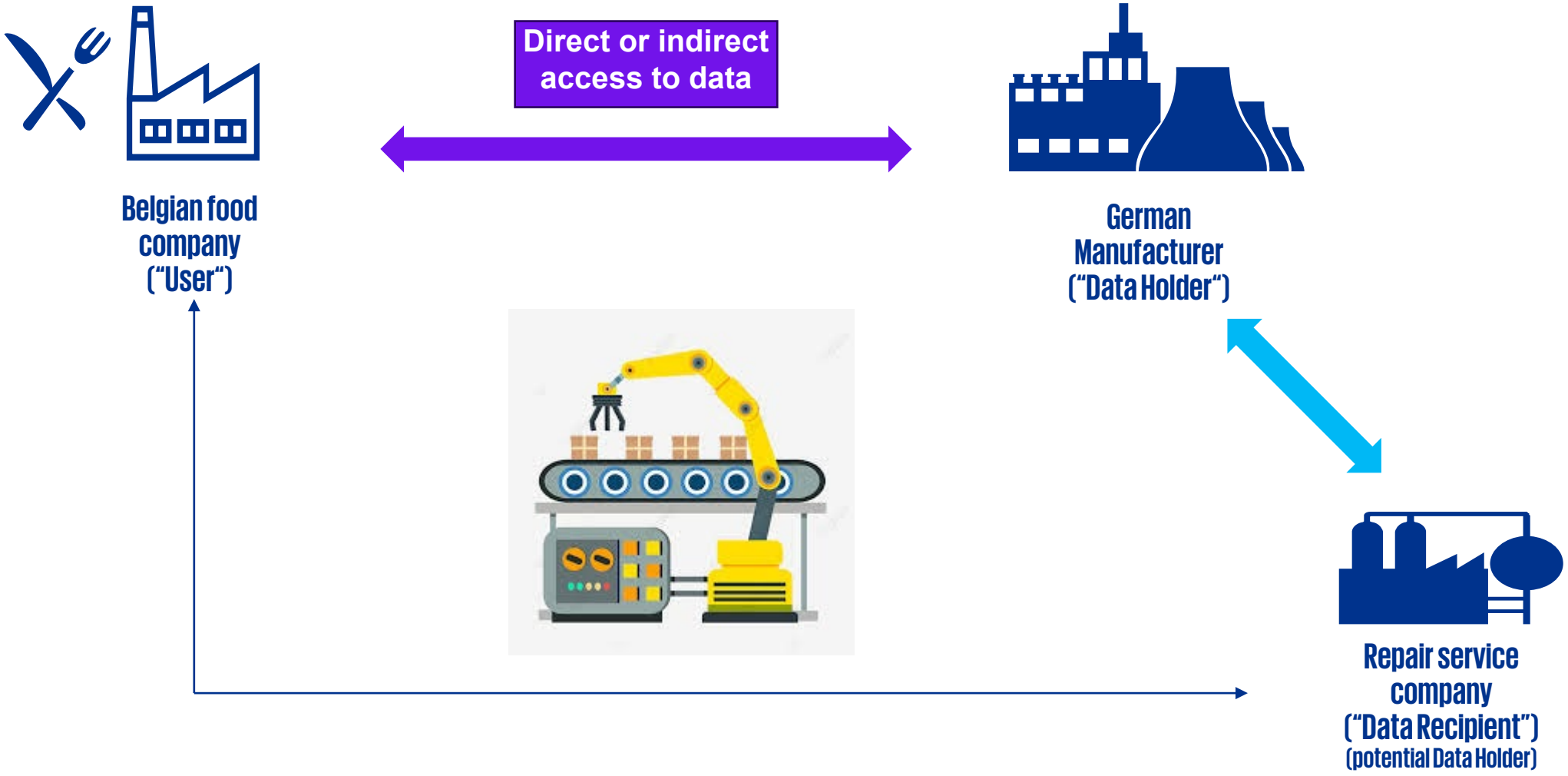
2.1. Scope: (Extra-)Territorial effects

Principle: placing/offering on the EU market

Extra-territoriality

- A manufacturer of a connected product and/or a provider of the related service established outside of the EU can also be in scope
- A user must be established in the EU to benefit from the rights under the Data Act

2.2. B2B & B2C IoT data sharing



2.2. B2B & B2C IoT data sharing: Main obligations

01

Access (by design)

- Direct & secure access to user where technically feasible, free of charge
    - Direct vs. indirect access
- Share data with third parties (portability)

02

Transparency

- **What**? Mandatory minimum information
- **When?** Prior to concluding contract for connected products/related services
- **Who?**
    - Seller, rentor or lessor of connected products
    - Provider of related services
- **How?**
    - In a clear & comprehensive manner
    - Data act notice?

03

Required contracts

- Between data holder & data user
- Between data holder & data recipient (third party)
    - FRAND-terms
    - Prohibition of unfair terms
        - Black list & grey list
        - All data, not only IoT-data
- Non-binding model contractual terms

2.2. B2B & B2C IoT data sharing: Protection of the interests of the data holder

Trade secret handbrake & safety handbrake

Prohibition to use data to develop competing products

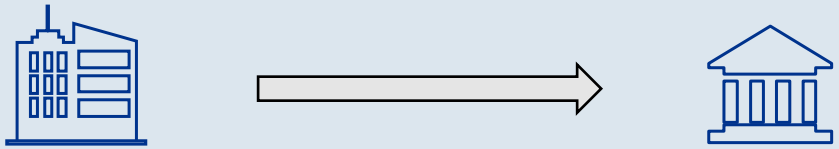
- Only applies for data of connected products, not for related services.

Compensation from third parties/data recipients

2.3. B2G data sharing

B2G data sharing

Public sector bodies may request data from companies



When can data be requested?

- **Public emergency** e.g. natural disasters, cyberattacks, pandemics, etc.
- **Other exceptional need**
  - To prevent or recover from emergencies
  - To fulfill a specific public interest task

Conditions & safegards

- Requests must be proportionate, specific and necessary
- Data limited to what is strictly necessary
- Transparency: purpose & legal basis must be communicated
- Protection of trade secrets and confidential information

Compensation

	Other companies (not micro and small companies)	**Micro and small companies**
Public emergency	Free of charge Public recognition	Reasonable remuneration Public recongition
Non-emergency situation	Reasonable remuneration	N/A (exempt from obligation to provide data)

2.4. How to prepare?

01

Determine whether in scope

- Assess whether your company is in scope
  - Size
  - Territoriality
- Identify and map connected products and/or related services
- Assess your role under the Data Act (user, data holder, data recipient)
- Identify the data in scope
- Impact analysis of new rules on business

02

Update (contractual) materials

- Data Act notice
  - Transparency and information obligations
- Drafting contracts
  - With user (B2B & B2C)
  - With data recipient (B2B)
    - Unfair terms
    - FRAND terms
- Reviewing and adapting existing data sharing/license agreements
- Reviewing and adapting general terms and conditions / terms of use

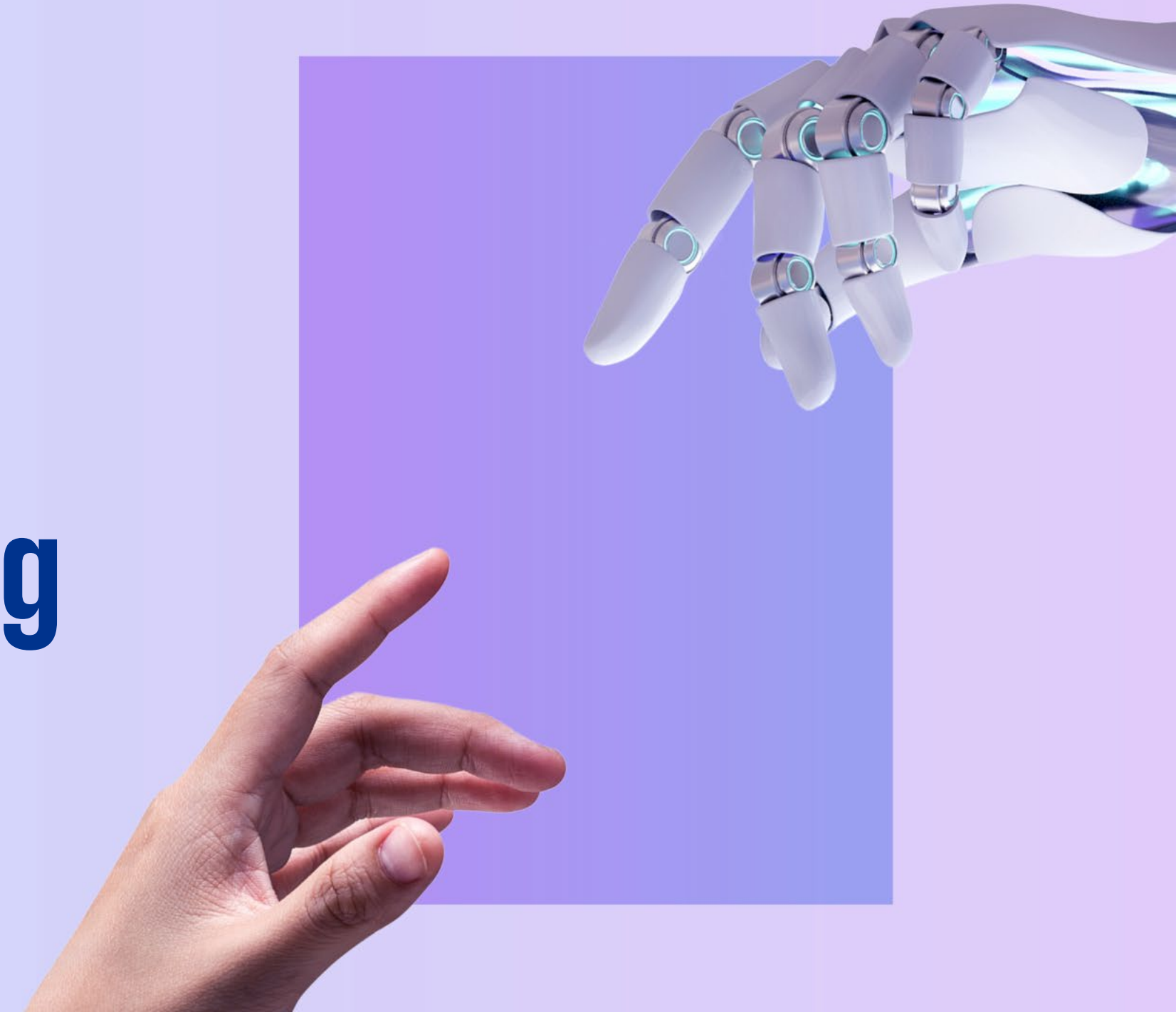
03

Handling data sharing requests

- Reviewing data governance
- Assess lawfulness of data sharing requests (B2C / B2B / B2G)
- Determine applicability of trade secrets handbrake

03

Data Processing Services



3.1. Data processing services – which providers are covered?

01

≈ Cloud services

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Storage as a Service
- Database as a Service
- Etc.

02

Excluded

- Non-production services for testing and evaluation purposes
- Traditional hosting services

.

03

Partially excluded

- Data processing services
  - Of which most of the main features have been **custom-built;** and
  - which are not offered at broad commercial scale via the provider's service catalogue

04

Territorial application

- Providers offering data processing services to customers in the EU
- Obligation to establish a legal representative for non-EU providers

3.2. Data processing services – Obligation to remove barriers

Take measures to enable customers:

- **To switch to** a data processing service covering **the same service type** but provided by a different data processing services provider
- To **switch to on-premises ICT-infrastructure**
- Where relevant, **to use several providers** of data processing services at the same time (in a **multi-vendor model**)

May not impose and shall remove pre-commercial, commercial, technical, contractual and organisational obstacles, which prevent customers from:

- Terminating the contract after max. notice period and successful switching
- Concluding new contracts with other providers
- Porting customer's exportable data and digital assets
- Achieving functional equivalence
- Unbundling data processing services

3.3. Data processing services – Contractual requirements

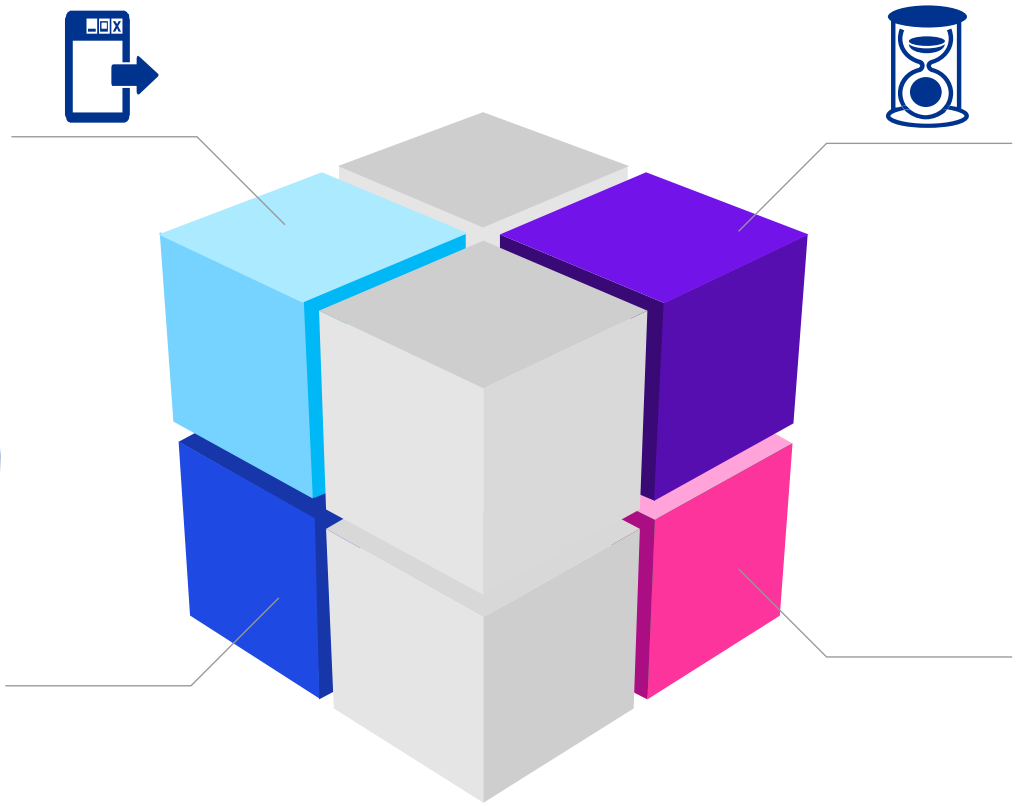
All contracts on data processing services need to include a number of specific clauses on switching between data processing services, including the following:

Obligation to support the customer's exit strategy

- To the respective contracted services
- Supply all relevant information

An exhaustive specification of:

- Digital assets and exportable data
- Categories of data specific to the internal functioning that are not portable (risk of trade secrets breaches)



Clear deadlines

- Notice period (max. 2 months)
- Transitional period (max. 30 days), but extendable up to 7 months
- Data retrieval period (min. 30 days)

Clause guaranteeing full erasure

- Data generated by the customer
- Data relating to the customer

Non-binding Standard Contractual Clauses

3.4. Data processing services – Transparency requirements

General information obligation:

In case of international access and transfer:

Information on procedures

Information on available procedures for switching and porting to another data processing service

Jurisdiction

- The jurisdiction to which the ICT-infrastructure deployed for data processing of their individual services is subject
- On the website of provider of data processing services

Up-to-date online register

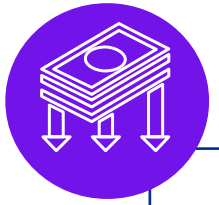
Reference to an up-to-date online register hosted by the provider of data processing services

- Details of all data structures
- Details of all data formats
- Relevant standards and open interoperability specifications

General description of TOMs

- General description of TOMs to prevent international governmental access or transfer of non-personal data
- On the website of provider of data processing services

3.5. Data processing services – (Pre)commercial requirements



Switching charges:

- **As from 12 January 2027:** complete abolition
- **Until 12 January 2027**: reduced switching charges (cf. actual incurred costs)

Obligation to provide clear information on the following topics:

- Standard service fees and early termination penalties
- Reduced switching charges that may still apply
- If switching is highly complex or costly or if switching is impossible without significant interference in the data, digital assets or service architecture

Information must be publicly available via a dedicated section on provider's website or in other easily accessible way

3.6. Data processing services – Technical requirements

IaaS providers

Obligation to take all reasonable measures in their power to facilitate that the customer, after switching to a service covering the same service type, achieves **functional equivalence** in the use of the destination data processing service

Obligation to facilitate the switching process by **providing capabilities, adequate information, documentation, technical support** and, where appropriate, the **necessary tools**

Other providers

Obligation to **make available open interfaces**, for the purposes of data portability and interoperability, to an equal extent to all their customers and the destination providers of data processing services **free of charge**

Obligation to ensure **compatibility with** common specifications based on **open interoperability specifications** or harmonized standards for interoperability (where published)

3.7. How to prepare?

01

Determine whether in scope

- Assess whether the (cloud) services you use or provide qualify as a data processing service
- Consider what must/can be switched (exportable data and digital assets)
- Consider (extra-)territorial effects

02

Update (contractual) materials

- Mandatory written agreement
  - Keep unfair B2B terms and mandatory contractual requirements in mind
- Reduced switching charges
  - No more switching charges as from 12 September 2027
- Information requirements
  - Available on website of data processing service provider
- Update relevant policies
  - TOMs

03

Technical/operational compliance

- Map data to align with portability requirements
- Make gap analysis against new requirements
- Develop internal procedure for switching requests
- Ensure security throughout the process
- Keep timescales in mind
- Consider technical functional equivalence requirements

3.8. International transfers

General

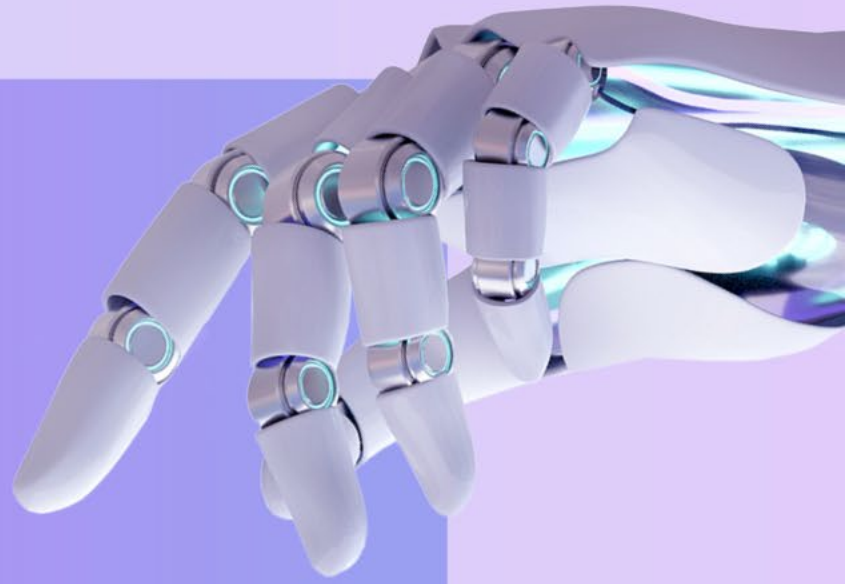
- **Scope:** non-personal data stored in EU by data processing services provider
- **Technical, legal and organisational measures**
  - Prevention of unlawful third country governmental access to data
- **Goal:** protection within EU “travels with the data” when accessed or transferred outside the EU

Third country request (legal order/judgement)

- Only if based on an **international agreement** between third country and EU
- If **no such agreement**: **conditions** to be fulfilled:
  - reasons and proportionality of order/judgement and request is specific
  - reasoned objection of addressee is subject to review
  - court/tribunal empowered to take into account legal interests of provider of data
- **If request is OK**:
  - minimum amount of data transferred
  - customer must be informed in advance

04

Enforcement and Sanctions

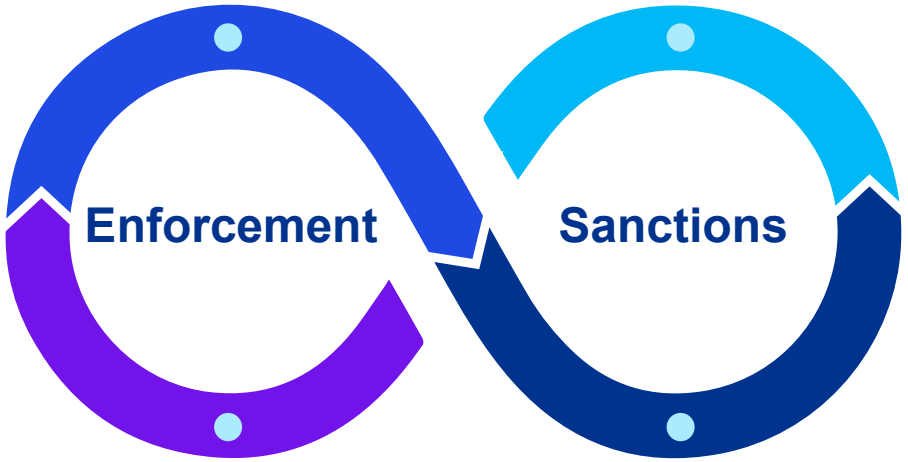


4. Enforcement and sanctions

Enforcement

- By national authorities

→ **Belgium:** not yet designated

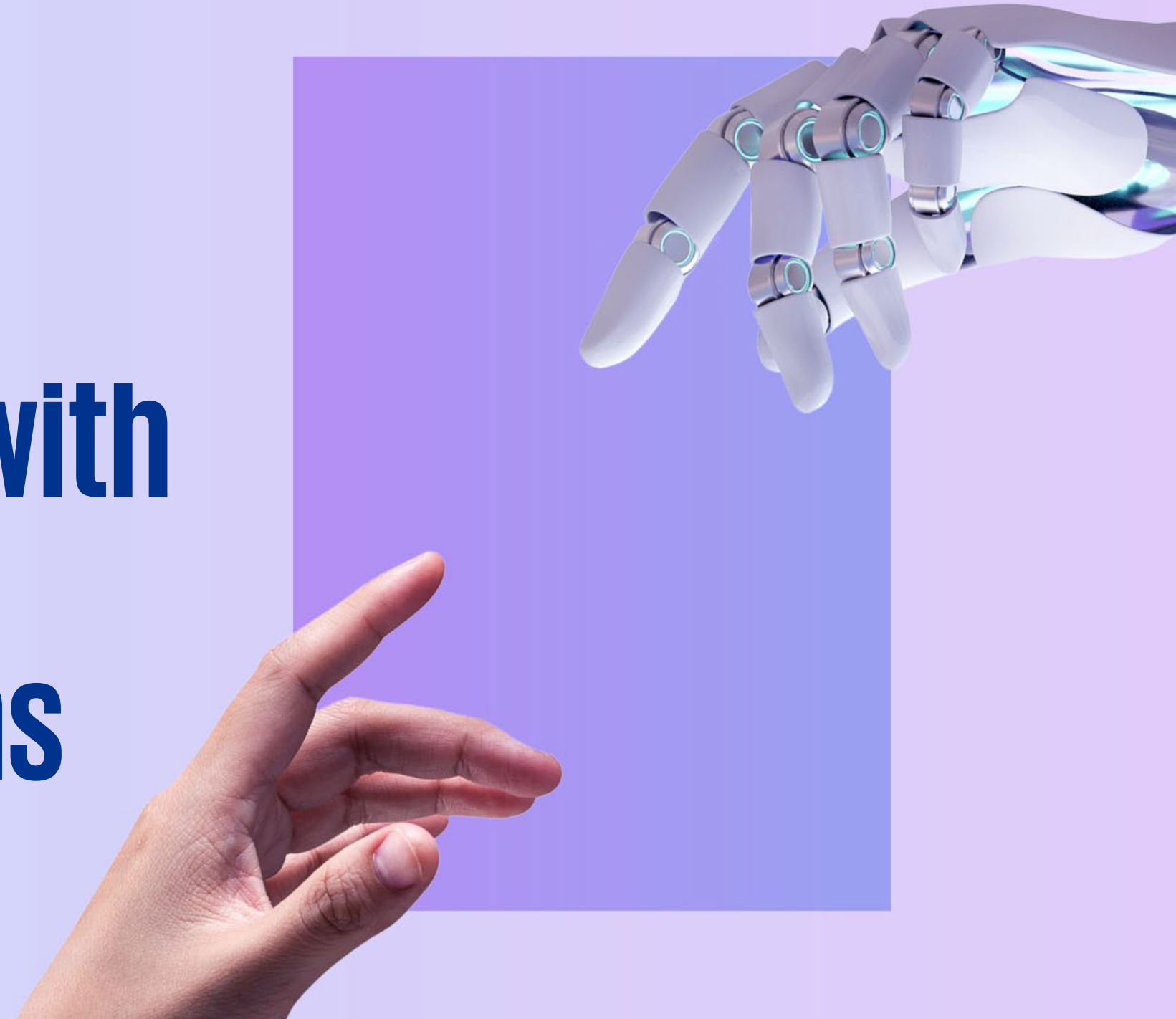


Sanctions

- Framework for penalties, but no exact fines or amounts are specified
  - Criteria for imposition of penalties

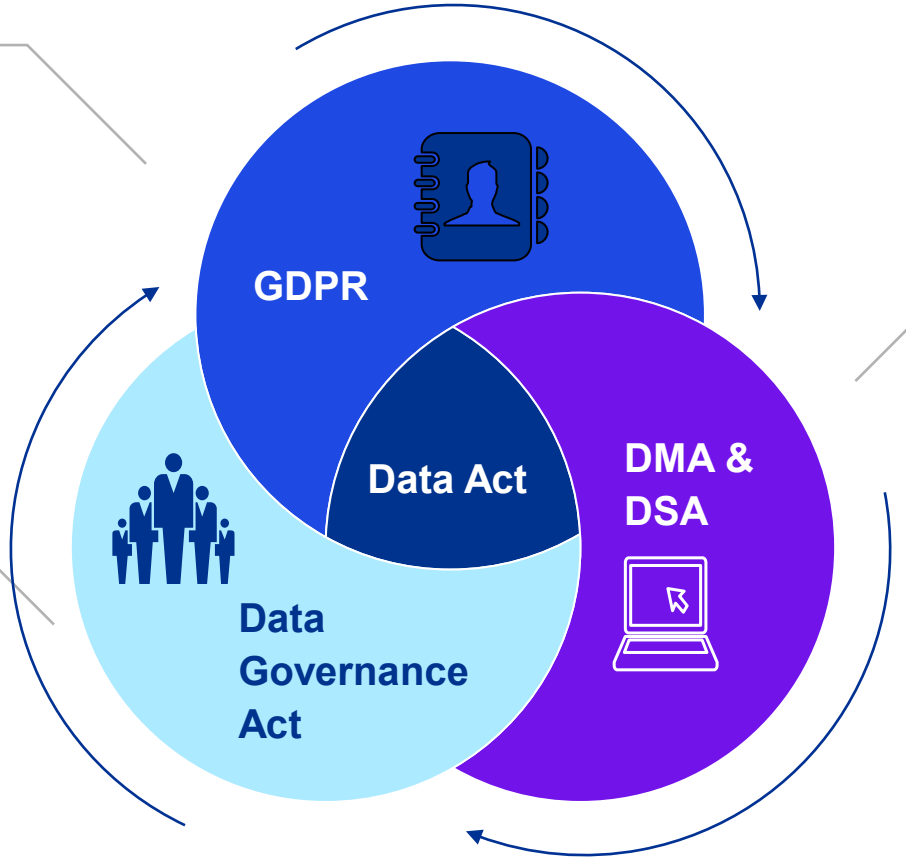
05

Interplay with other regulations



5. Interplay with other regulations

- Complementary nature
- Overlap in practice
  - Right to data portability
- GDPR prevails if conflict

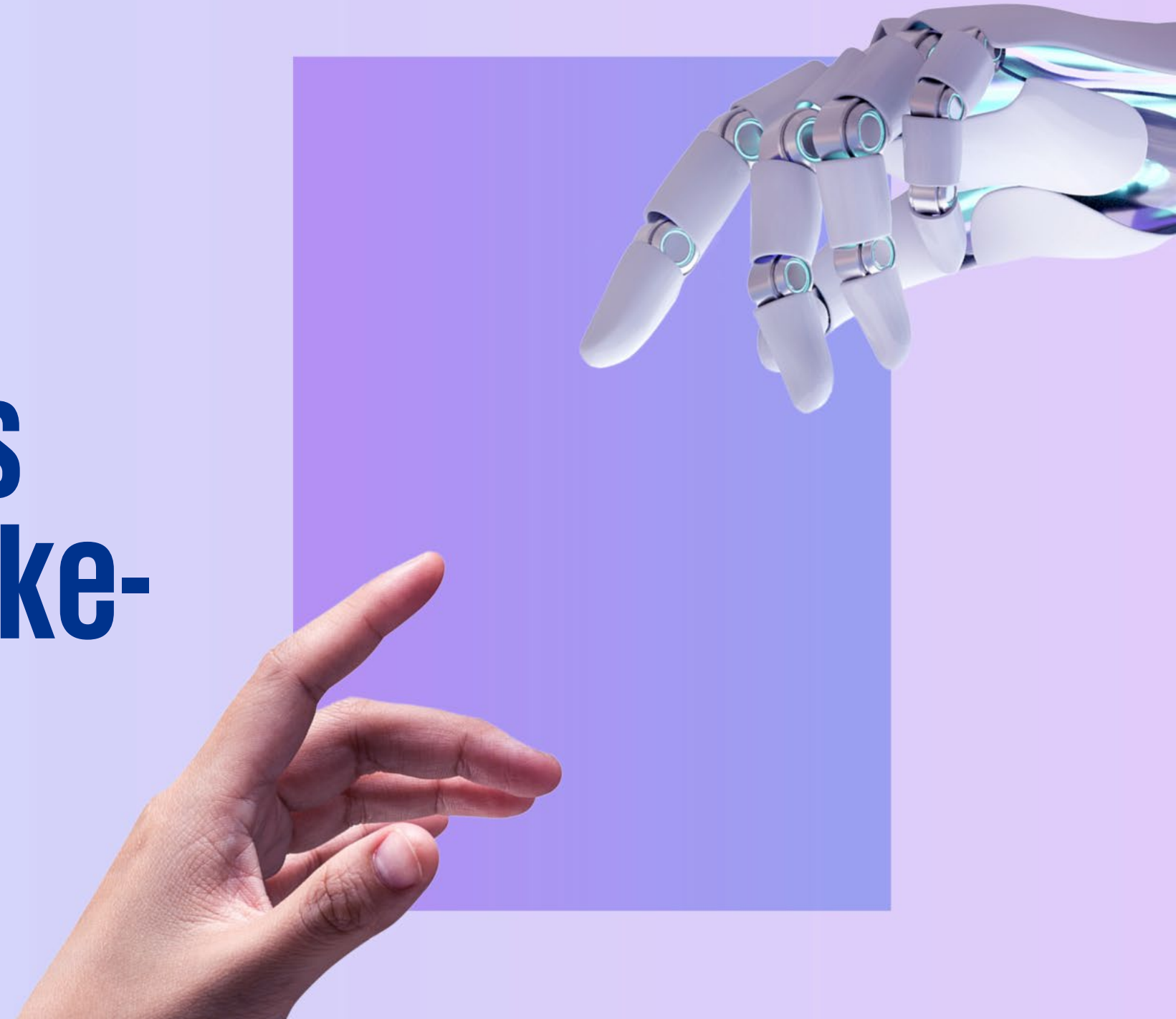


- Gatekeeper exemptions

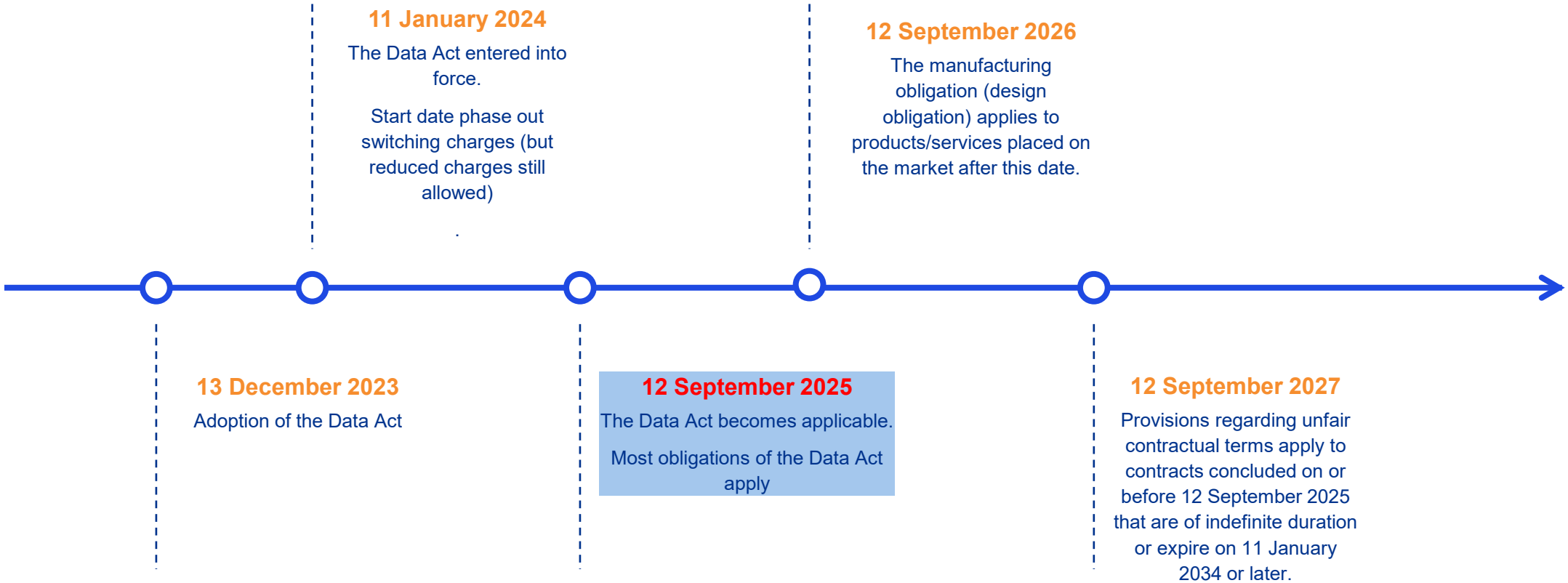
- European strategy for data
- Complementary roles

06

Next steps and key take-aways



6.1. Timeline



6.2. Key take-aways

New opportunities

The Data Act will change the way data is shared and the way in which customers can switch data processing services

New (compliance) challenges

The Data Act will also create legal and technical headaches for those in charge of compliance

Assess the scope

Investigate by which parts of the Data Act your organisation is affected and which rights and/or obligations this brings along

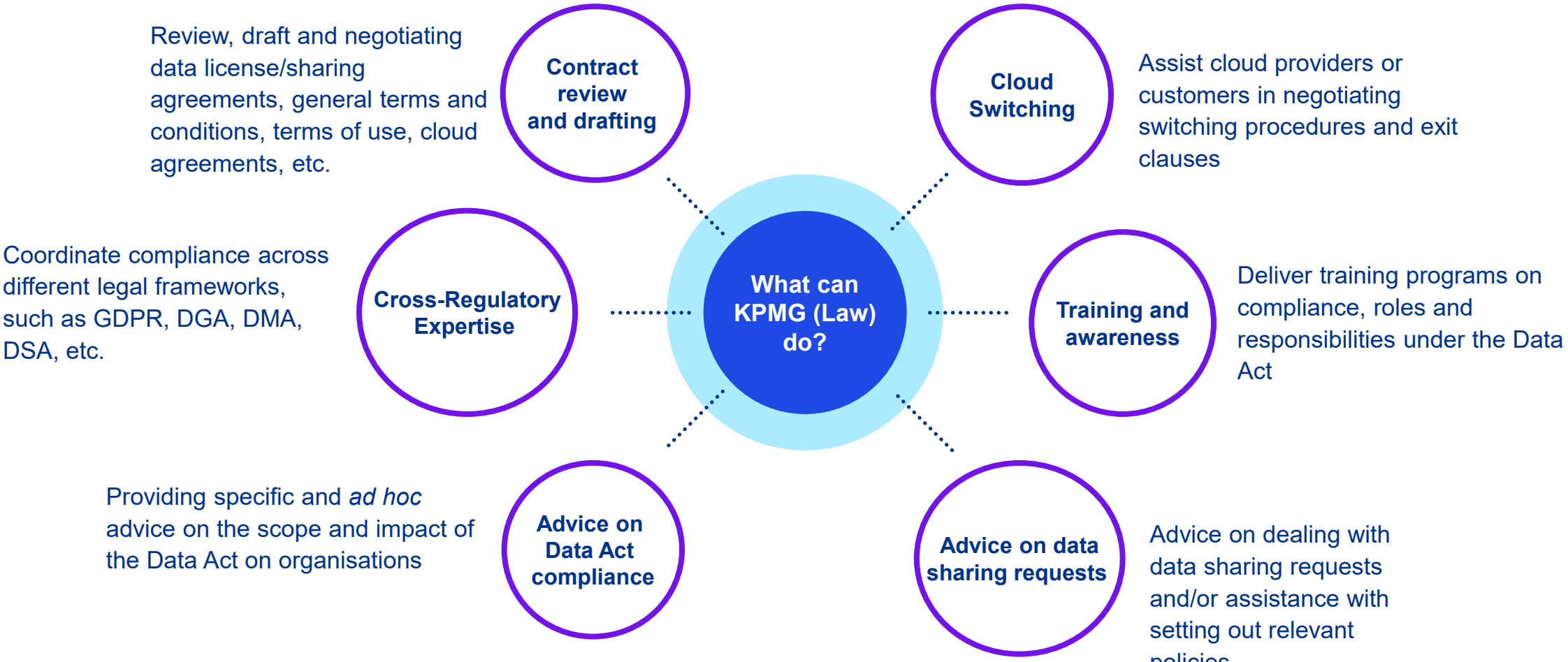
Draft/update documentation

Where relevant ensure the relevant contractual documents and notices are drafted and/or updated

Update/put in place TOMs

Where applicable, ensure your organisation’s processes and measures allow to comply with the Data Act

6.3. KPMG (Law) can help you



Contacts

Raf Schoefs

Senior Counsel
Technology, IP & Data

E-mail: rschoefs@kpmglaw.be

Tel: +32 475 42 93 36

LinkedIn:

Laura Vanuytrecht

Counsel
Technology, IP & Data

E-mail: lvanuytrecht@kpmglaw.be

Tel: +32 498 24 11 35

LinkedIn:

Thank you for attending

kpmg.com/be