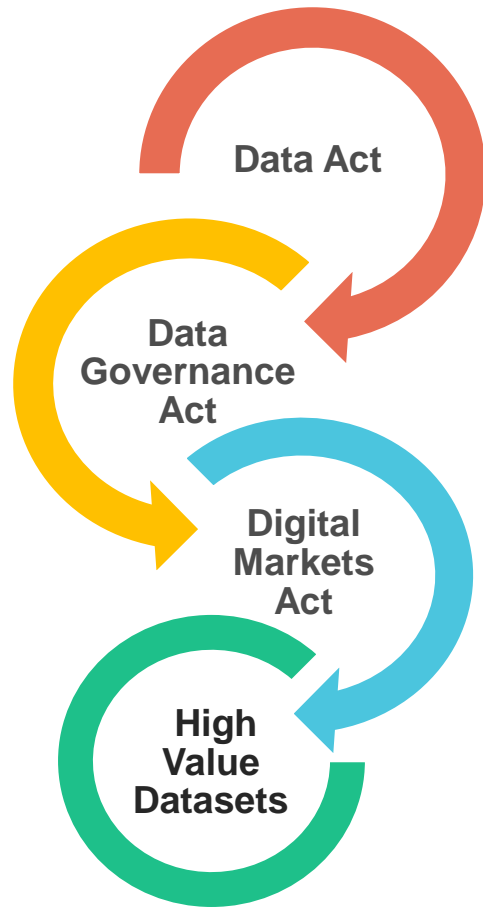




Some elements of the Data Act

European Commission
June 2025

Cross-sectoral legislation to enable the EU Data Strategy



Overall aim: **Single EU Data Space** (free flow of data for innovation, research, etc)

Ensure **FAIRNESS** in the allocation of data value among the actors of the data economy (Data Act).

Ensure **TRUST** in data transactions (Data Governance Act)

Tackle imbalances caused by the **MARKET POWER** of gatekeepers (Digital Markets Act)

Unleash the socio-economic potential of data as a raw material for **INNOVATION**, in particular for **SMEs** (HVD)

1. Legislation complements and builds on the rights existing under the **GDPR**
2. **Sectoral legislation** can impose further requirements

Data Act

Entry into application 12 September 2025



Better access to **IoT data**

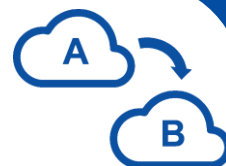
Rules for IoT data also frame data sharing in other sectors



Tackle **contractual unfairness** in B2B data sharing



Make **business data available** for public admins (B2G)



Easier **switching** between cloud services



Facilitate data flows through **standards** and **interoperability**, in particular for data spaces

Components of the Data Act (I)



Chapter II on B2B and B2C data sharing in the context of IoT

Users of IoT objects can access, use and port data that they co-generate through their use of a connected product



Chapter III on B2B data sharing

Clarifies the data-sharing conditions wherever a business is obliged by law to share data with another business



Chapter IV on unfair contractual terms

To protect all businesses, in particular SMEs, against unfair contractual terms



Chapter V on B2G data sharing

Public sector bodies will be able to make more evidence-based decisions

Components of the Data Act (II)



Chapter VI on switching between data processing services

Providers of cloud and edge computing services must meet minimum requirements to facilitate interoperability and enable switching



Chapter VII on unlawful third country government access to data

Non-personal data stored in the EU is protected against unlawful foreign government access requests.



Chapter VIII on interoperability

Participants in data spaces must fulfil criteria to allow data to flow within and between data spaces.



Chapter IX on enforcement

Member States must designate one or more competent authority(ies) to monitor and enforce the Data Act

Chapter III: Mandatory B2B data sharing

Rules for when a business ('data holder') has a legal obligation (EU or national law) to make data available to another business

Notably, the data-sharing terms and conditions must be fair, reasonable and non-discriminatory.

Data holders that are obliged to share data may request *reasonable compensation*

Chapter V: B2G data sharing



Data held by private entities may be essential for a public sector body to undertake a task of public interest

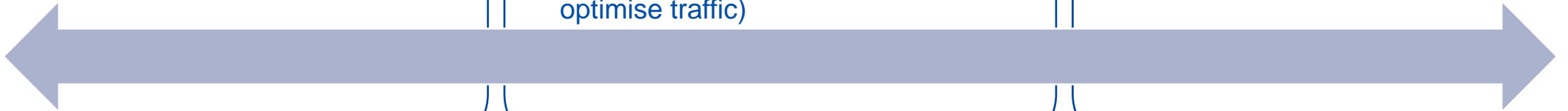


Public sector bodies to access data where there is an exceptional need

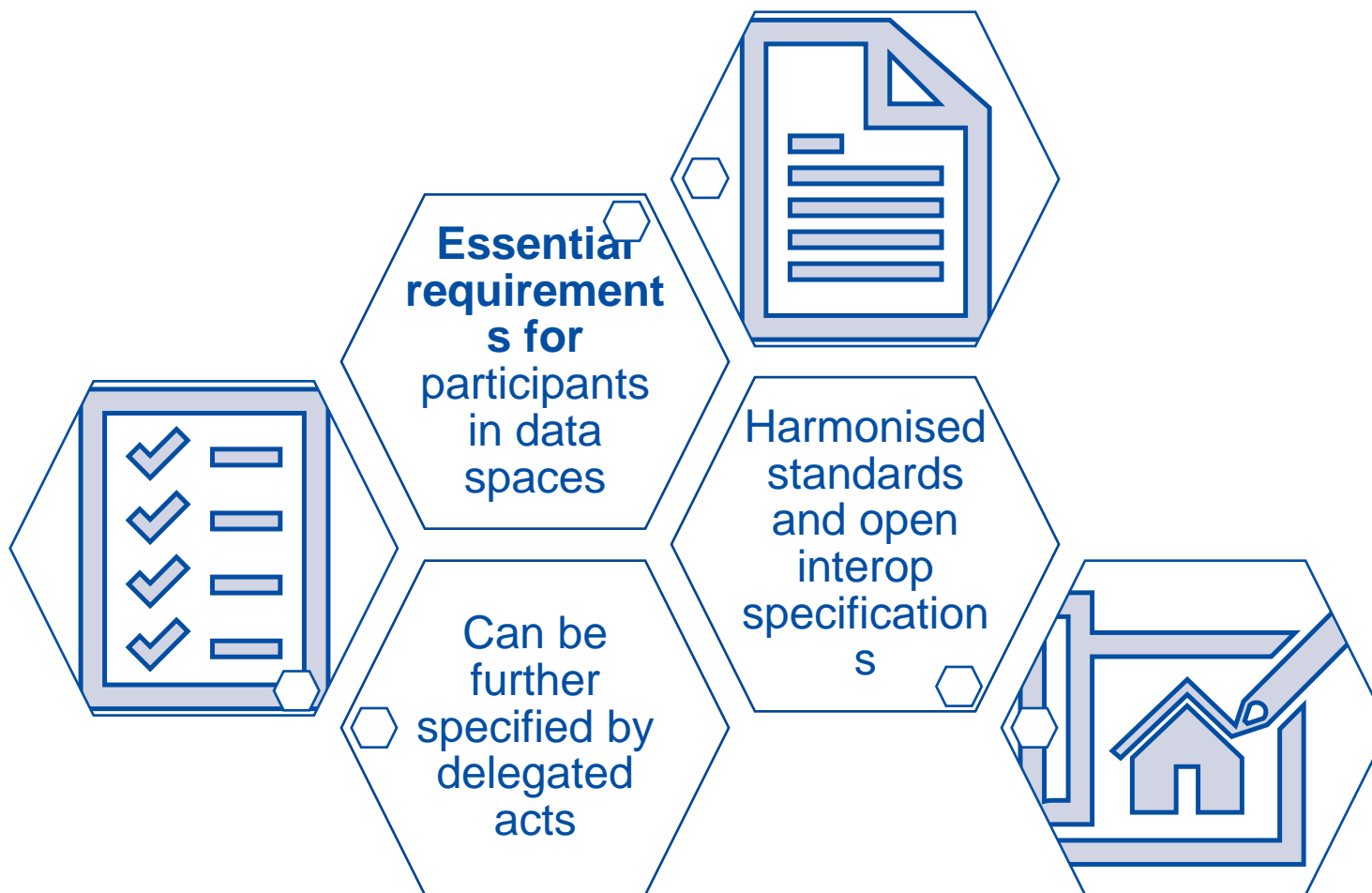
- Necessary for a public interest task, notably to improve evidence-based decision making
- Both emergencies and non-emergencies (e.g., GPS data to optimise traffic)



All data are in scope, with a focus on non-personal data.



Chapter VIII: Interoperability



Chapter IX: Enforcement

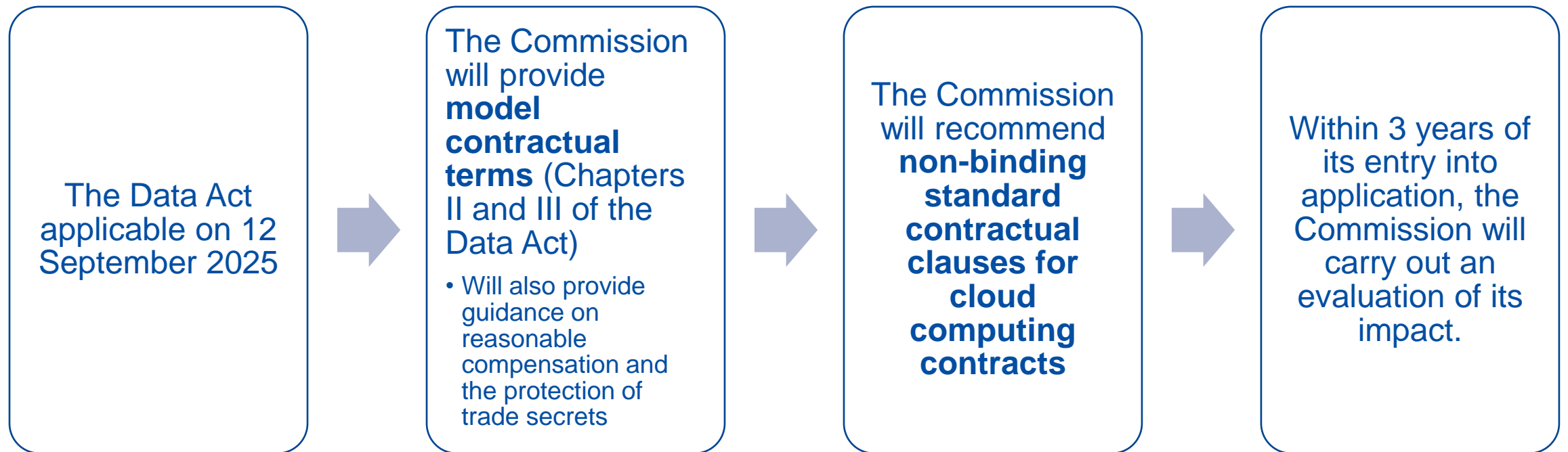
Member States to designate 1+ competent authorities

The Commission will maintain a public register

Member States may set up certified dispute settlement bodies

- Parties are free to address any dispute settlement body – either in the Member State in which they are established or in another

Next steps



Thank you



© European Union 2024

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.