



Data Governance Act and the Data Act

LES France Conference

17 October 2023

Szymon Lewandowski
DG CONNECT, Data Policy and Innovation Unit
European Commission

Creating a single European market for data

European Data Strategy

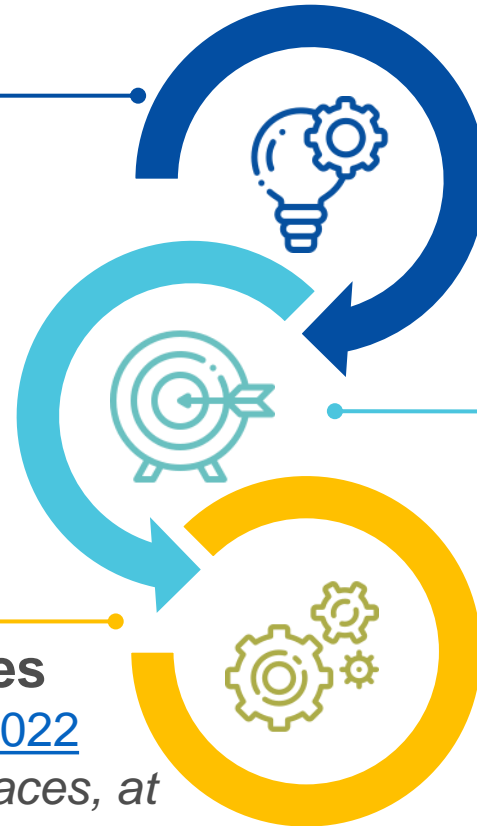
- [Published Feb 2020](#)
- *Genuine* internal data market
- Built on EU values and rules

Common European data spaces

- [Staff Working Document – Feb 2022](#)
Overview development data spaces, at request European Council
 - ✓ Horizontal aspects (concept, legislation, EU programmes/funding)
 - ✓ Sectoral/domain-specific initiatives

A cross-sectoral legislative framework

- [Data Governance Act](#) – July 2022
- [Data Act](#) – early 2024 (estimated entry into force)
- [Implementing Act on High-value datasets](#) (Open Data Directive) – December 2022



Data Governance Act

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022, entry into application 24 September 2023)

Pillar 1:

Re-use of **closed data** held by **public sector bodies**

- **European single access point to public sector's non-open data**

=

European register for protected data held by public sector – ERPD

Pillar 2:

Framework for new **data intermediaries** in the Single Market:
Data broker

- **EU register of data intermediation services**
- **Common logos for data intermediaries**

Pillar 3:

Corporate and Individual **data altruism** for purposes of general interest

- **EU register**
- **Common logos for data altruism organisation**
- **Common European consent form**
- **Data altruism rulebook**

Pillar 4:

Co-ordination and interoperability:
European Data Innovation Board

Re-use of categories of protected public data

Complementary to Open Data Directive:

- Shall cover data that can only be used under certain conditions, because others have rights on that data (personal data, trade secrets, confidential business information, IP).
- Building on national access regimes: where re-use happens, it should do so in a harmonised manner, **subject to conditions**.
- Leaves room for MS, but aims to **create at least one contact point (single information point)** an interface for re-users that seek to re-use protected public data.

EUROPEAN SINGLE ACCES POINT

serves as a searchable electronic register of the information compiled by national single information points.

Data sharing intermediaries

Design principles and requirements for **novel intermediaries for B2B and C2B data sharing**:

- Support and boost voluntary data sharing preserving control over the data by companies and individuals.
- Cannot monetise on the data companies share through them; they have to comply with strict requirements to ensure this neutrality and avoid conflicts of interest.
- **Data intermediary services** function as neutral third parties that connect individuals and companies on one side with data users on the other.

EU REGISTER OF NOTIFIED DATA INTERMEDIARY SERVICES

a regularly updated public register of all data intermediation services providers providing their service in the Union (Art. 11 (10))

Individual & corporate data altruism

Data altruism entities have the option to register as 'Data Altruism Organisations recognised in the Union' if meeting certain requirements.

- Individuals and companies could share their data for the common good, without direct reward.
- European data altruism consent form to facilitate the collection of data.
- Each member states shall keep and **regularly update a public national register of recognised data altruism organisations.**

EU REGISTER OF RECOGNISED DATA ALTRUISM ORGANISATIONS

a public Union register of recognised data altruism organisations for information purposes

Data Act – main topics covered



Better access to IoT data



Rules for IoT data also frame data sharing in other sectors



Tackle contractual unfairness



Make business data available for the common good



Easier switching between cloud services



Facilitate data flows through technical standards and interoperability

Use of data in an Internet of Things context (B2B & B2C)

Before



User
(individual or company)

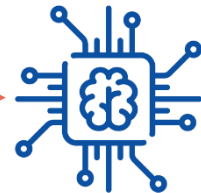
Limited application of portability

Little to no interaction



Manufacturer

Various obstacles for data sharing
(technical, legal, etc.)



Third Party

After



User
(individual or company)

Enhanced access and transparency

Granting access to data for improved services



Manufacturer

Clear and fair rules on data use

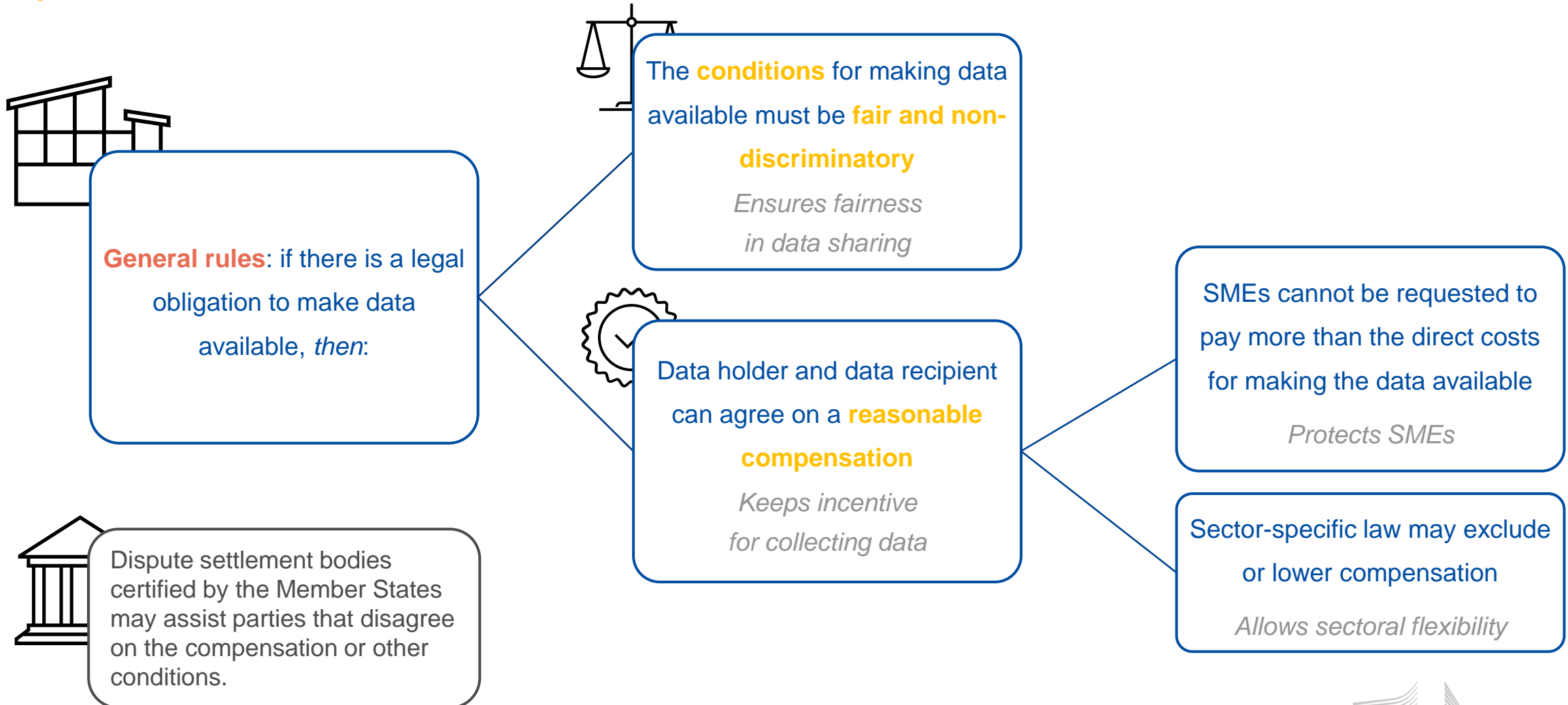


Third Party

‘Emergency handbrakes’

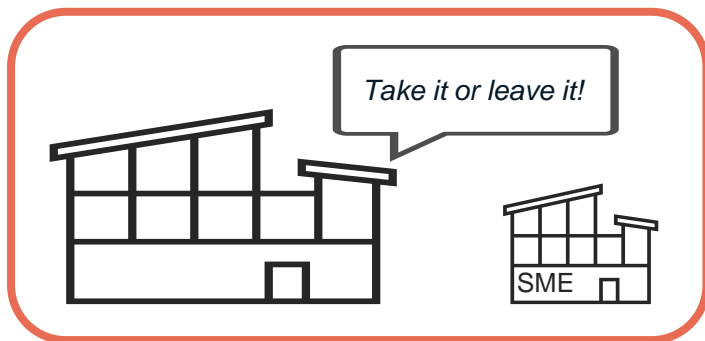
- **Trade secrets handbrake:** trade secrets holders can refuse requests for access or sharing of data where this could cause serious economic harm and where this is based on objective, justifiable factors.
- **Security handbrake:** data holders can refuse requests based on security considerations only in very specific circumstances, on a case-by-case basis.
- Safeguards against misuse:
 - Data holders must demonstrate the necessity for using the mechanisms
 - Competent authorities must be notified when handbrakes are applied
 - Appeal and dispute settlement procedures
 - Commission review (Art 41)

CHIII - Conditions for making data available between businesses

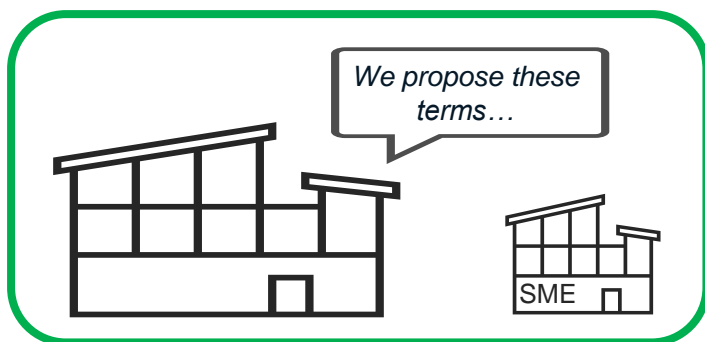


CHIV - Unfairness test for B2B contracts:

Unfair contractual terms unilaterally imposed on enterprises are non-binding.



From this situation...



...to an actual negotiation.

General provision on unfairness concerns clauses which

- Grossly deviate from good commercial practice in data access and use and are contrary to good faith and fair dealing.

Listed clauses that are always/presumed unfair (examples)

- Exclude or limit liability of the imposing party
- Prevent from using contributed data or exploiting their value
- Unreasonably short termination conditions

Model contractual terms

- Developed and recommended by the Commission to assist parties in drafting contracts based on fair terms.

Chapter V (B2G) – mechanism for access to private sector data

Data is requested based on an exceptional need:

- a) to respond to a public emergency (*all types of data and includes micro and small companies*)
- b) Where data is necessary to fulfil a task in the public interest and the data is otherwise unavailable (*only non-personal data*)

Special procedure applies to **cross-border requests** (Art 22)

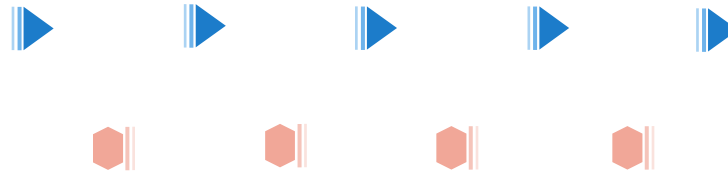
Stronger requirements apply to personal data (anonymisation, notification to the DPA) and **trade secrets** (protective measures to be agreed).

Data is **destroyed after use**
*subject to national transparency laws

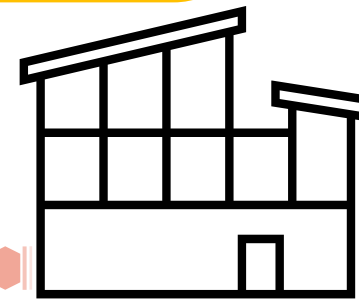


Public sector body

Public sector body requests data based on an exceptional need



Private sector body makes data available for the **purpose, period** described in the request



Private sector

Existing and future [compliance, reporting] sectoral obligations (incl. for law enforcement purposes) continue to apply

Public sector body, Commission, ECB or Union bodies

Compensation: free for public emergencies (except for micro and small companies), reasonable compensation in all other cases

*Exemption made for national statistical offices where unable to purchase data

CHIX - Enforcement

Each Member State designates one or more competent authorities to carry out the function of application and enforcement

- 'Data coordinators' now act as the single point of contact
- Can be already existing bodies or structures
- DPA's competences over data protection are respected
- Sectoral authorities' competences respected



What will the Data Act change?



Harmonized rules on data access and use to **unlock the potential of the EU's industrial data**



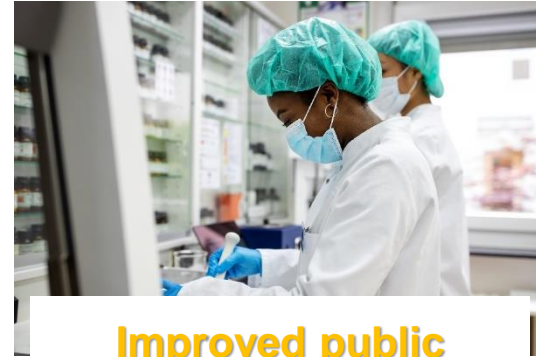
New data-based business opportunities



Empower individuals and companies using connected products and related services



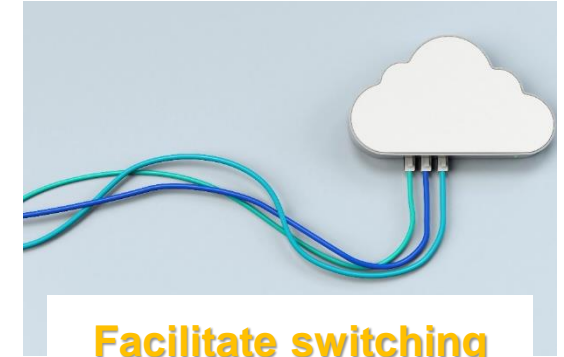
More transparency and control as well as better decisions over data



Improved public service delivery, including effective response to public emergencies



Better and more efficient public services and policies

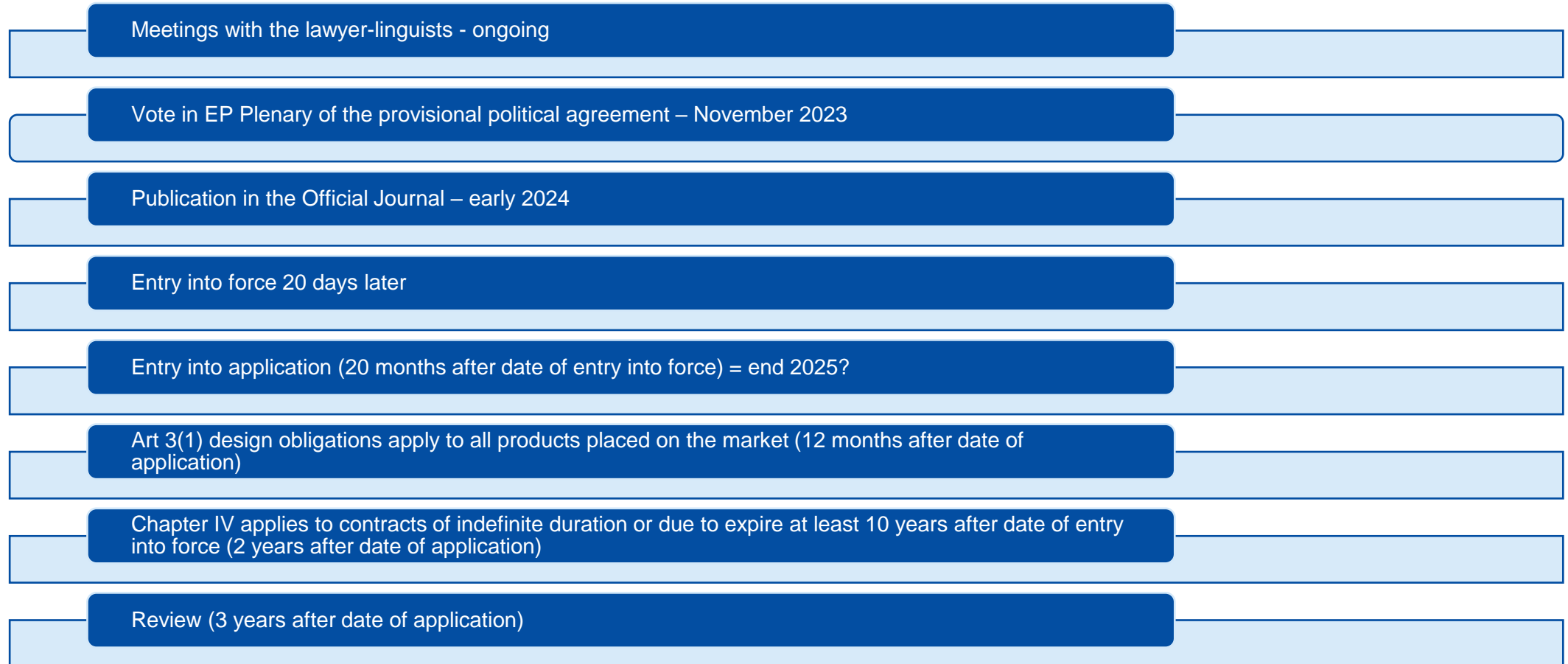


Facilitate switching for cloud users



Multi-vendor, interoperable and federated cloud/edge services market

Timeline (pursuant to Article 41)



Thank you