Krogeruksen Datasymposium 2023

Yhteistyössä

Teknologiateollisuus

krogerus

What should companies take into account when applying Data Act?

Pascal Belmin
Vice President, Head of EU Aviation &
Regulatory Affairs
Airbus Group

What should companies take into account when applying the Data Act?

Pascal Belmin
Head of EU Regulatory and Aviation affairs
Airbus Brussels

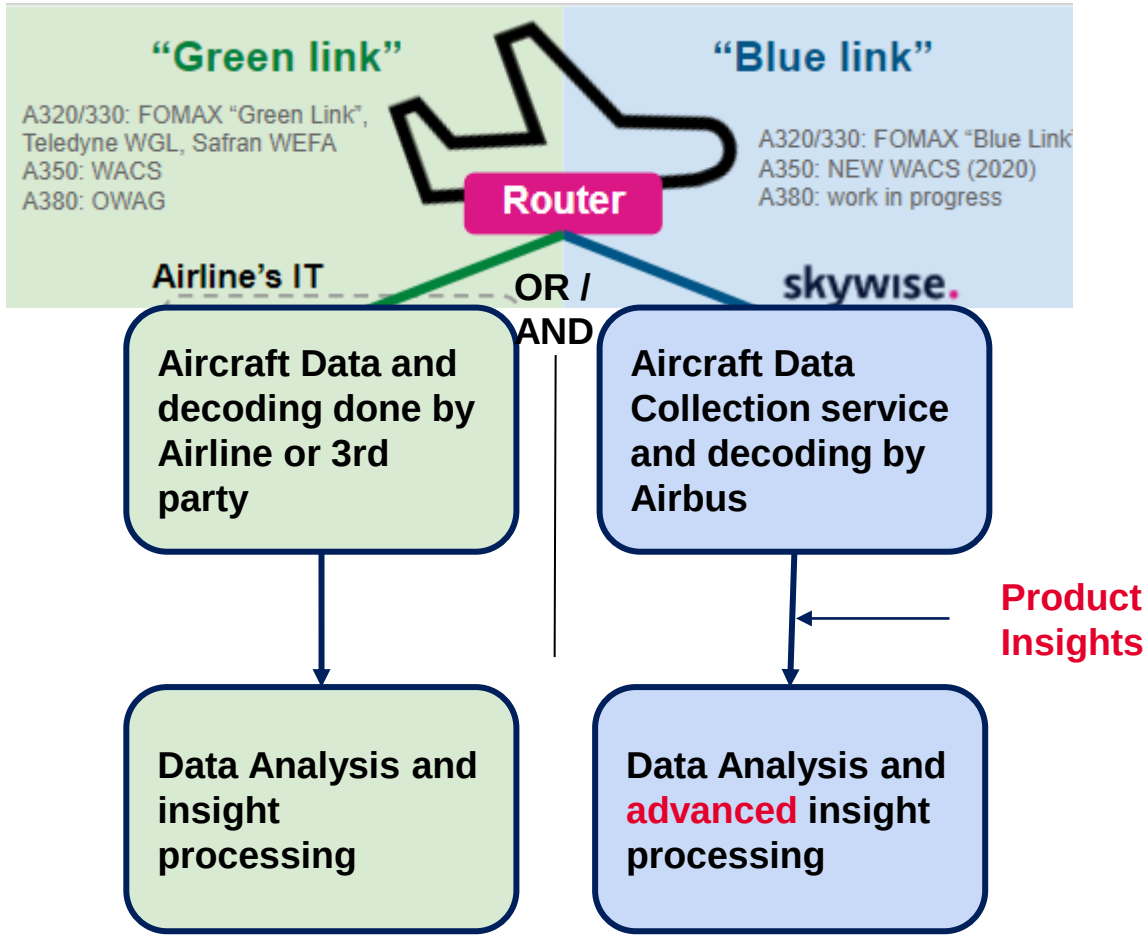
Introduction

- Support data sharing and the principle of the Data Act. Issues lied in avoiding dissemination of most sensitive data in order to preserve innovation incentives in the EU.
- Unlike other digital regulations (e.g. AI Act), limited sectoral angle in the Data Act - industries have different issues and focus areas.
- Intervenes before voluntary data sharing initiatives (e.g. sectoral data spaces) have fully produced effects.
- Questions remain on interpretation: clarifications expected from EU Commission beginning 2024.
- Main focus here on B2B data sharing chapters in industrial environment + overview of certain other Chapters.

Internal company organisations
Functions and departments impacted

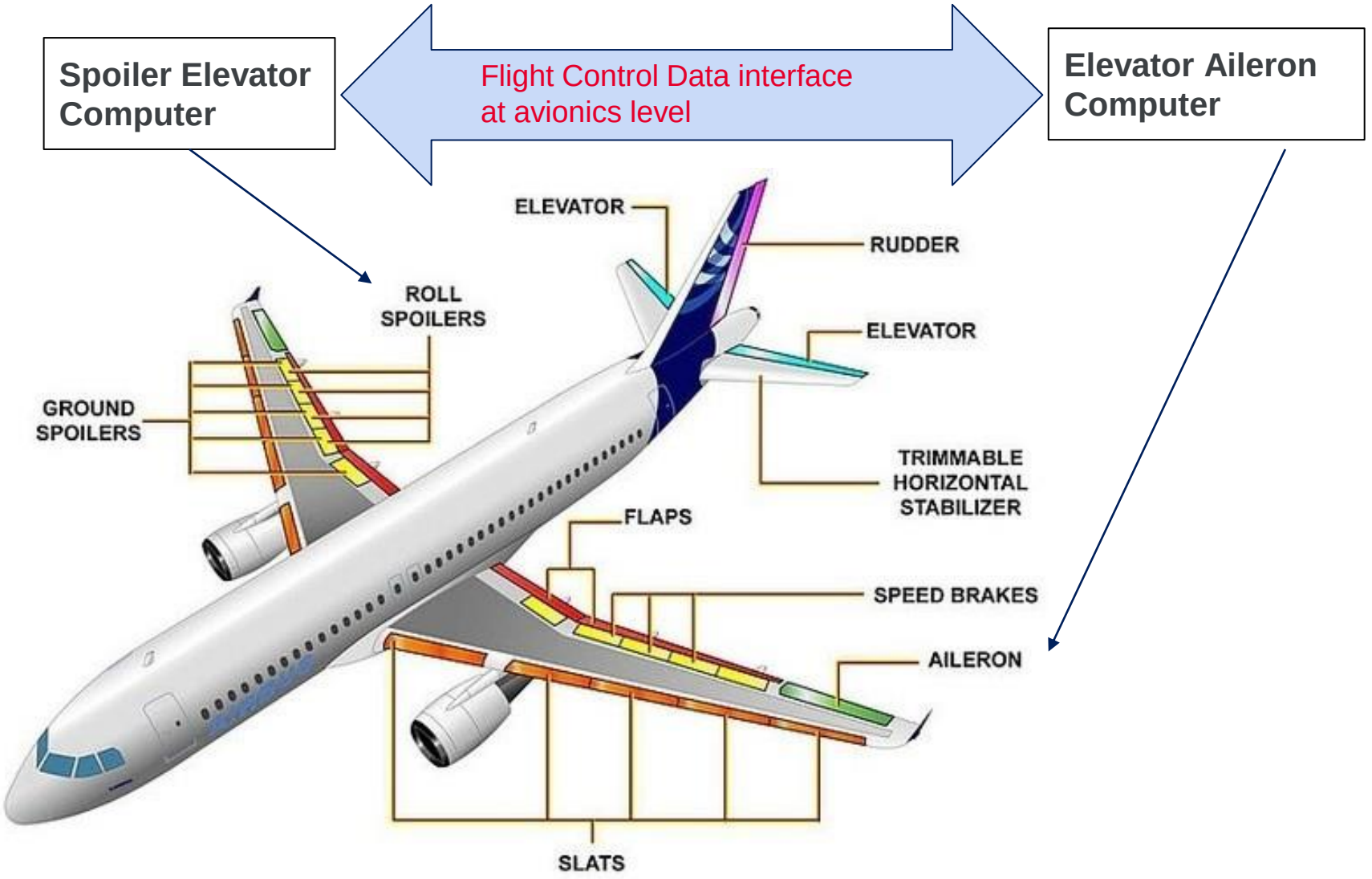
- Digital / IM teams
- Design office (eg. obligations related to product design)
- Production / engineering (e.g. production chain)
- Sales (pre-sale information requirement, contract content and implementation)
- After sales and services
- Legal / Compliance
- Public affairs

B2B Data sharing - use case



- Very significant amounts of data already shared + we do not have more data than airlines
- Green data is airworthiness (safety) related and available to airlines (by default not to us) - fully decodable, already allows for 99.7% a/c reliability
- Blue (enhanced) data extracted upon airline demand for predictive maintenance service: data itself not readily available to Airbus. Data collection and processing requires investment. Involves significant costs.

Identifying and avoiding dissemination of excessively sensitive information



- **To be placed in context of environmental roadmap: technologies and product data will relate significantly to this. Maintain technological edge and competitive advantage.**

Main B2B Data sharing obligations

Key principles:

- Obligation for manufacturer to:
  - **Design and manufacture products and "related services" so that** product data and related service data are easily, securely, *free of charge, in a comprehensive, structured, commonly used and machine-readable* format, and, where relevant and technically feasible, directly accessible to the user.
  - **Provide prior information** to the user (eg. about data that can be generated or stored by the product or service made available) including in relation to "related services"

- **Where data cannot be directly accessed by the user** from the connected product or related service, data holders shall, upon user request, make **readily available data** accessible to the user (same conditions as above + same quality as is available to the data holder, continuously and in real-time.

- **Users** may make available data directly or indirectly to **data recipients in the Union**, subject to safeguards. Compensation possible in certain cases.

- Among the lawful data use purposes is lawful **reverse engineering**.

To be understood within precise definitions and frameworks set out below

Geographical scope and application in time

- **Geographical scope**: the Data Act (all chapters, not just B2B sharing) applies to:

(a) **manufacturers** of connected products and **providers** of related services ***placed on the market in the Union, irrespective of their place of establishment***;

Applies to non-EU manufacturers and related service providers under conditions below re: users and data recipients.

(aa) **users** of such connected products or related services **in the Union ;**

In our understanding: does not apply to sales to customers *established outside the EU*, even if products are then brought or used in the EU (e.g. mobile phone, aircraft, etc.). To be confirmed.

(a) **Data holders**, ***irrespective of their place of establishment***, that ***make data available to data recipients in the Union***;

(b) **Data recipients in the Union** to whom data is made available.

Does not apply to data recipients outside the Union. Was understood to avoid obligations to transfer data to recipients outside the EU - **implementation? Contractual provisions, but which controls?**

- **Entry into force and application in time (article 42)**

  - Generally, application 20 months after entry into force (20th day after OJ publication)
  - But regarding article 3(1) (obligation by design) one additional year before application: **no retrofit of existing products**

Data in and out of scope

- Exemptions:
  - Personal data & privacy,
  - Data Act **does not apply to or pre-empt voluntary arrangement** for exchange of data between private and public entitiesdefence, national security, etc.)
  - Data Act does not apply to areas **falling outside the scope of EU law**, and in any event **does not affect competences of Member States** in **public security, defence or national security**.

- Which data in and out of scope of Data Act?
  - **IPR exclusion**: *Data Act is without prejudice to Union and national legal acts providing for the protection of intellectual property*.
  - **Raw and processed data are in scope**, i.e. product data which are **not substantially modified**: **raw data** (primary data **without any processing**) and **pre-processed** data (to make it understandable and useable, eg. for wider use-cases by determining a physical quantity or quality or the change in a physical quantity, such as temperature, pressure, flow rate, audio, pH, liquid level, position, acceleration or speed). Does not impose an obligation on the data holder to make substantial investments in cleaning and transforming the data.
  - **Only readily available data is in scope**: product data and related service data that a data holder lawfully obtains or can lawfully obtain from the product or related service, *without disproportionate effort*, *going beyond a simple operation* (Article 2.1e)
  - **This excludes** data generated by the use of a product ***where the design of the product does not foresee such data to be stored or transmitted outside*** the component in which they are generated or the product as a whole. The Regulation should thus not be understood as an obligation to store data on the central computing unit of a product.

⇒ Underlying transverse principle: the manufacturer is free to design its product to ensure non availability of overly sensitive data - product data limited to *"data that the manufacturer designed to be retrievable"*. But this data would not be accessible to the manufacturer: impact on innovation?

Data in and out of scope

- Which data in or out of scope of Data Act? (continued)
  - **Information derived** from such data is out of scope:
    - *outcome of additional investments into assigning values or insights from the data, in particular, by means of **proprietary, complex algorithms, including those that are a part of proprietary software**, **should not be considered to fall within the scope of this Regulation** and consequently not be subject to the obligation for a data holder to make it available to a user or data recipient, unless agreed otherwise between the user and the data holder. Such data could include, in particular, information derived by means of **sensor fusion**, which infers or **derives data from multiple sensors**, collected in the connected product, using **proprietary, complex algorithms and may be subject to intellectual property rights***.

- **Sectoral legislation** could be introduced to outline further specificities.

Related services

- **Related service** (article 3 and 4)

  means a digital service other than an electronic communications service, including software, which is ***connected with the product at the time of the purchase*** in such a way that ***its absence would prevent the 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 product*** (Article 2.3)

  - We would interpret that even the second part of the sentence relates to the **indispensable** services (examples: fridge & pizza oven).
  - **Consequence: downstream added value services and predictive maintenance are <u>not</u> a related services.**

  ⇒ **Importance to determine services which for your company are in or out the scope: non related services not subject to any obligations**.

Protection of trade secrets and “emergency brakes”

- Safeguards built in to protect sharing of overly sensitive data

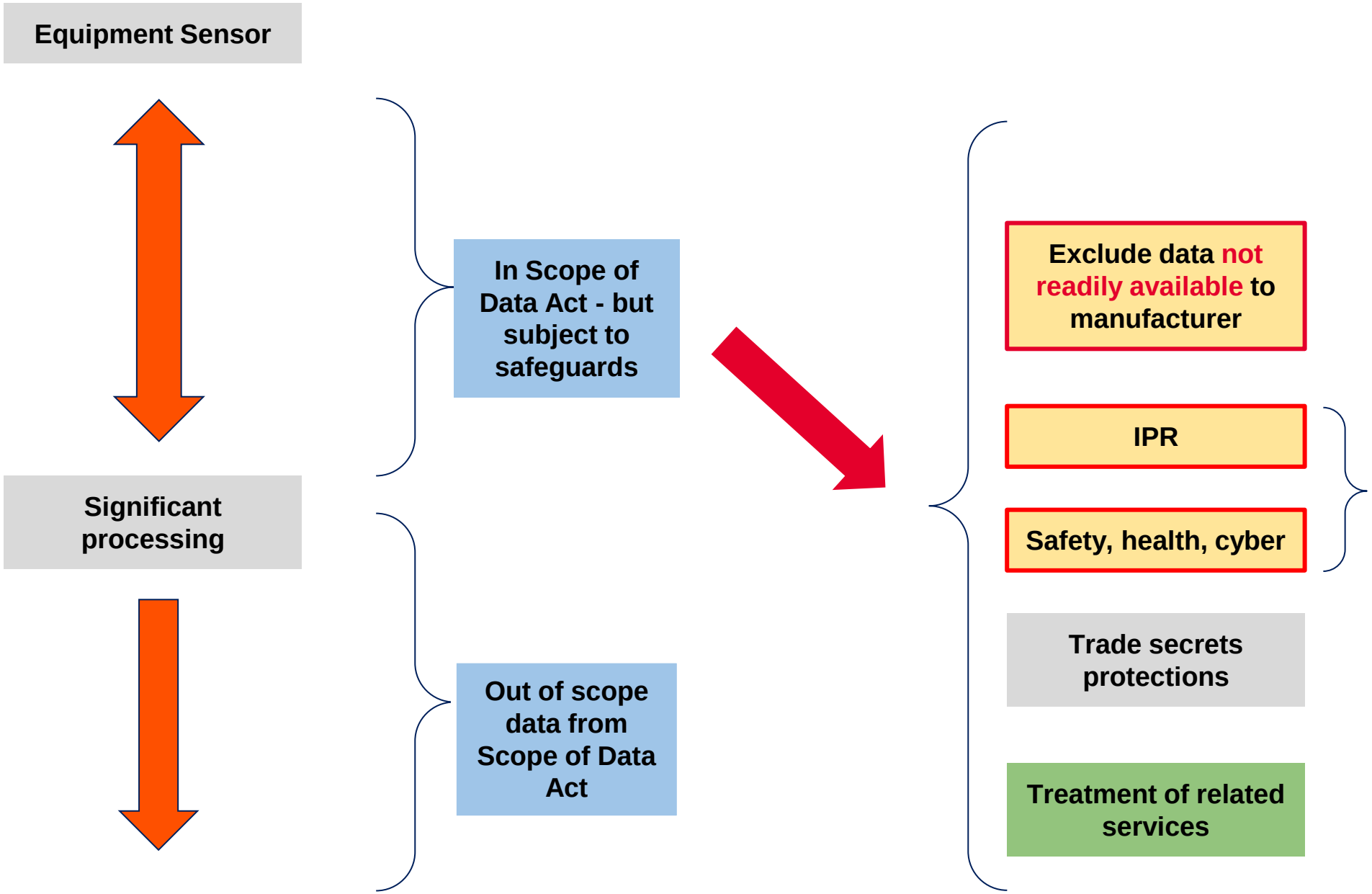
  - **Article 3**: “by design”.

  - **Article 4**:
    - Under the data holder / user contract, data sharing that could **undermine product security requirements** and impact seriously **health, safety and security can be avoided**. Subject to dispute settlement. Notification of national authority. Involvement of **sectoral** authority possible.
    - **Trade secrets protection, including *ex ante***: disclosed only if all necessary measures are agreed upon, defined and properly implemented. Possibility to suspend data sharing otherwise, under oversight of national authority. Dispute resolution always possible.

  - **Articles 5 to 8**:
    - Relates to data transfers to third parties and data recipients in the Union (except gatekeepers), subject to trade secrets protections similar to above.

Protection / advocacy strategy based on matrix approach

[Airbus Amber]



Making Data Available to Public Sector Bodies Based on Exceptional Need (Chapter V)

- Relevant Definitions
  - **‘public sector body’** means national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies;

  - **‘public emergency’** means an **exceptional situation**, **limited in time** such as public health emergencies, emergencies resulting from natural disasters, as well as human-induced major disasters, including major cybersecurity incidents, negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, financial stability, or the substantial and immediate degradation of economic assets in the Union or the relevant Member State(s) and which is determined or officially declared according to the relevant procedures under Union or national law;

- Need to **demonstrate exceptional need**
- Based on **justified request**
- Exceptional need always **limited in time and scope**
  - When data ***necessary to respond to public emergency*** and the public sector is unable to obtain such data by alternative means in a timely and effective manner under equivalent conditions (Article 15.1.a) – Concerns non-personal and personal data. Free of charge except for SMEs and micro enterprises
  - When a public sector body, acting on the basis of Union or national law, necessitates specific data to fulfill a ***specific task in the public interest***, **and** *has exhausted all other means* at its disposal to obtain such data (Article 15.1.b) – Concerns non-personal data only. Fair remuneration.

- **To be noted that this concerns potentially all company data, not only product or service generated data.**

Switching Between Data Processing Services (Chapter VI)

- Removal of obstacles for **effective switching between providers of data processing services**
  - Aims to enable customers to switch to another service (same service typebut different provider) or to use several providers of data processing services at the same time.
  - Providers of a data processing service shall not impose and shall remove pre-commercial, commercial, technical, contractual and organisational obstacles to switching.

- The Act sets out **precise contractual terms** concerning switching between providers of data processing services

- Data Act sets **information obligation of providers of data processing services** (especially on procedures for switching and porting to the data processing service + reference to an up-to-date online register)

- **Gradual withdrawal of switching charges including data egress charges**
  - After 3 years post entry into force, providers of data processing services shall not impose any switching charges on the customer for the switching process, including data egress charges.
  - Within 3 years of entry into force, providers of data processing services may impose reduced switching charges, including data egress charges, on the customer for the switching process.

- Data Act also covers the more technical aspects of switching.

International governmental data access and transfer (Chapitre VII - Article 27)

- **Providers of data processing services** to take all **measures** measures to **prevent international and non EU governmental access and transfer** of EU non-personal data where this would **conflict with Union or national law.**

- **Data request enforceable** if and within conditions of **international agreement** with third country concerned.

- **Otherwise, if risk of conflict of law, the provider of data processing services can only accept transfer if:**
  - Non-EU legal system requires the request to be specific, proportionate and sufficiently linked to the data requested.
  - Subject to appeal
  - Taking in due consideration the interest of the EU data provider.
  - Opinion of national body or authority can be requested, in particular regarding trade secrets, commercially sensitive data and IP rights. Opinion compulsory if can affect defence or national security interests.
  - Commission to develop guidelines on the above.
  - In any event data provider must provide as little data as permissible under the request.
  - Provider must inform data holder, save exception