LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

The Data Act Proposal – Praise and some criticism for an ambitious project

Prof. Dr. Matthias Leistner, LL.M. (Cambridge)
Ludwig Maximilian University Munich


MORE DATA
MORE VALUE
MORE DIGITAL
That easy?!
#EUDataAct #DigitalEU

Agenda

I. Introduction: Data Act – Objectives, Overview and the Regulatory Framework

II. Data Act: a Closer Look …

1. Data Access, Use & Sharing (of IoT Data)
2. B2B Fairness Test
3. B2G Data Access for Exceptional Needs
4. Switching between Cloud & Edge Services
5. Database sui generis right, Art. 35

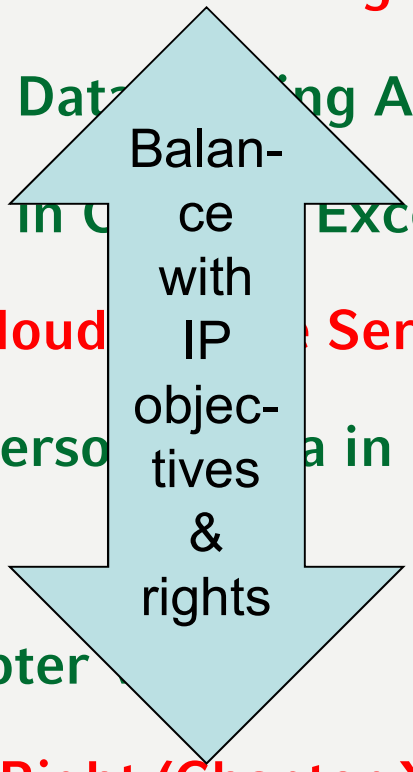
III. Summary and Perspective

Data Act – Overview

1. B2C and B2B Data Access & Sharing (Chapter II & III)
2. Fairness Test for B2B Data Sharing Agreements (Chapter IV)
3. B2G Data Access/Use in Cases of Exceptional Need (Chapter V)
4. Switching between Cloud & Edge Services (Chapter VI)
5. Safeguards for Non-Personal Data in International Contexts (Chapter VII)
6. Interoperability (Chapter VIII)
7. Database sui generis Right (Chapter X – Art. 35)

Data Act – Overview

1. B2C and B2B Data Access & Sharing (Chapter II & III)
2. Fairness Test for B2B Dat… …ng Agreements (Chapter IV)
3. B2G Data Access/Use in C… …Exceptional Need (Chapter V)
4. Switching between Cloud… … Services (Chapter VI)
5. Safeguards for Non-Perso… …a in International Contexts (Chapter VII)
6. Interoperability (Chapter …
7. Database sui generis Right (Chapter X – Art. 35)



The Regulatory Framework

- **Open Data Directive** (G2B data sharing)
- **Free Flow of Non-Personal Data** (inter alia: CoC for Cloud Switching)
- **GDPR** (Personal Data, including data access and portability, Art. 22)
- **Sale of Goods Directive** (Goods with digital elements = IoT products)
- **Digital Contents Directive (post-contractual data access and portability in Art. 16 (4))**
- **Unfair Terms Directive** (B2C)
- **Digital Markets Act Proposal**
- **Digital Services Act Proposal**
- **Data Governance Act Proposal**
- **AI Act Proposal**
- **Trade Secrets Directive**
- **Database Directive**

The Regulatory Fram ork

- **Open Data Directive** (G ata
- **Free Flow of Non-Pers** ud Switching)
- **GDPR** (Pe)
- **Sale of Good** = IoT products)
- **Unfair T**
- **Digital**
- **Digital Ser**
- **Data G**
- **A**
- **Trade Secr**
- **Database**

Coherence & legal certainty as genuine challenges

Overlaps?!

Art. 4: Right of users to access and use data generated by the use of products or related services

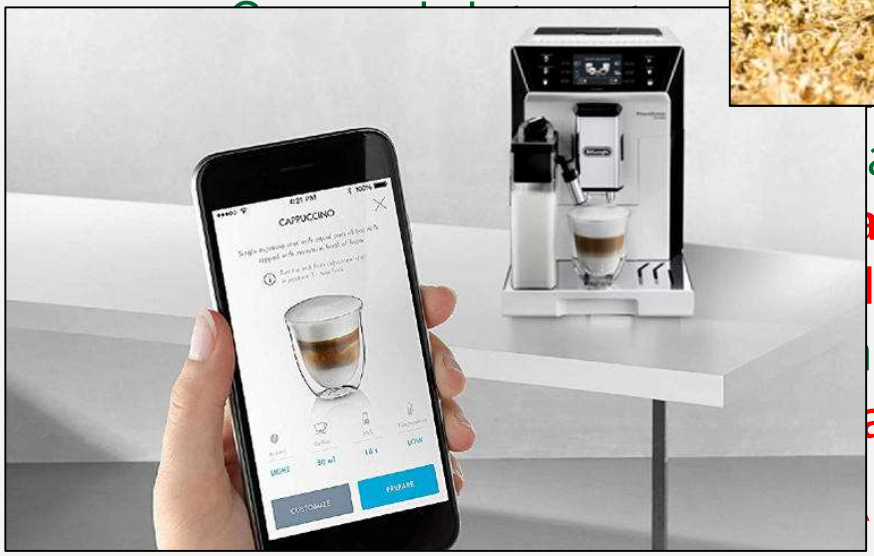
- **Scope**: Data generated by the use of a product or related service
  - Refers to **IoT products and 'incorporated' services**
    - Other **services** not covered
    - Why? Comprehensively covered by the Digital Markets Act?
    - But: this solely addresses **gatekeepers…**
  - Covered data categories: **volunteered and observed data**
    - **But: not inferred, 'contextualized' or 'standardized' data**
- **User: Business users** and **consumers**
  - Contractual relationship: sale/lease/rent agreement
    - **Use of non-personal data solely on the basis of a contractual agreement (= factual allocation!)**
- **Addressee:** Data holder (not necessarily manufacturer)
  - **Exclusion of micro or small enterprises (Art. 7)**
- **= 'Sector'-specific right for ALL IoT products – B2C & B2B**

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Data Acc

Art. 4: Right of users to a
produ

- **Scope**: Data generated b
  - Refers to **IoT produc**
    - Other **Services**: 'ou
    - Comprehensively c
    - But: addresses sole



ale/lease/rent agreement

ata solely on the basis of a contractual
llocation!)

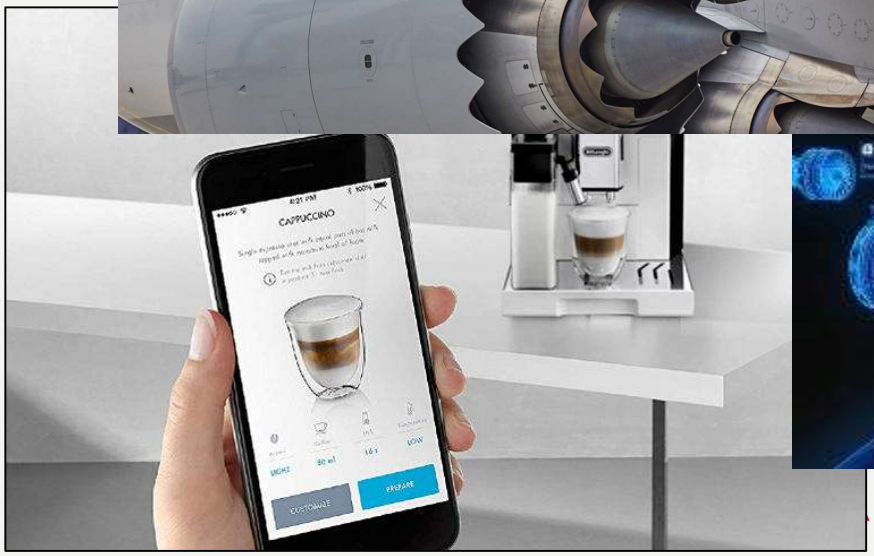
ecessarily manufacturer)

all enterprises (Art. 7)

LL IoT products – B2C & B2B

Art. 4: Right of users to ac
produ

- **Scope**: Data generated b



contractual

LL IoT products – B2C & B2B

Art. 5: Right to share data with third parties

- 'Upon **request by a user**, or **by a party acting on behalf of a user**, the **data holder shall make available the data** generated by the use of a product or related service **to a third party**'
  - = **User's right** to authorise and request data sharing with third party
- **Gatekeepers** (DMA) not as eligible third parties
- **Agreement** between **data holder** and **third party** specifying conditions of making data available: **FRAND terms** and **compensation**
- **= Central role of the user**
  - **but: Agreement between data holder and third party necessary**
  - **…and: what is the *ratio* for this governing role of the user when non-personal data are concerned (b2b)**

Overlap and balancing questions

- **Relation to trade secrets: obligation to guarantee confidentiality**
  - Scope of the proposed rights: Access and ***use****? (see* already Leistner/Antoine/Sagstetter, Big Data, 2021, p. 435 ff.)
  - **NB: trade secrets are not (only) about confidentiality!**
    - = Factual **exception** to Trade Secrets Directive?
    - But: Would this be justified 'across the board'?
- **Relation to database sui generis right**: see general provision, Art. 35
- **Relation to the GDPR**: Any processing of personal data has to be based on legal basis acc. to Art. 6 GDPR (or Art. 9 GDPR)
  - **Remarkable: While the 'interface' to relevant IP rights is envisaged and certain balance foreseen, the GDPR structure remains 'untouched'.**
- **Objective of fostering aftermarkets from a competition-law based perspective (but: in competition law this would only justify compulsory licenses in relation to market dominant undertakings)**
  - **Data Act: Prohibited** for user and third party to develop a **product that competes with the product from which the data originate**
  - **Convincing and sufficient approach?**

Cheaper prices for aftermarket services and reparation of their **connected objects**.

A factory robot breaks down.

TODAY	TOMORROW
Only the manufacturer can access the data, leaving no alternative for the company but to call them for repairing.	*The user could request that a repair service that may be cheaper also gets access to the data.*

New opportunities to use services relying on access to this data.

A farmer has equipment from different manufacturers (tractor, automatic irrigation system).

He cannot outsource the data analytics of its different equipment, the data is locked with each manufacturer.	*He could receive customised advices from a company gathering data from the different equipment.*

Better access to data collected or produced by a device.

A bar owner wants to serve better coffee, and the coffeemaker company wants to improve its product.

Only the company can access the data produced by the machine to design the next generation of coffeemakers but the bar owner cannot access information such as the quantity and temperature of water or coffee strength.	*The Data Act clarifies that both parties can access all data collected by the machine.*

Summary

- **Ambitious approach**
  - Entire IoT sector: **horizontal rules**
  - But at the same time: **one particular** case group
- **Access problems** primarily addressed as regards **individual level use data**
- **Access for competitors** to complete sets of **aggregated data** necessary for establishing workable **competition in aftermarkets or complementary markets**
  - Data Act facilitates primarily **occasional** and **selective data sharing** (e.g. for repair services)
  - **Not** designed for **large-scale data sharing**: third party would have to '**collect**' every dataset individually …
  - Some real bottlenecks (in regard to **standardized & contextualized inferred data** are not addressed either.
- **Factual allocation of non-personal data to user of IoT products!**
  - **Bilateral agreements** as key element (but: lacking standards)

Database sui generis right, Art. 35

Art. 35 – Databases containing certain data

In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, **the sui generis right** provided for in Article 7 of Directive 96/9/EC **does not apply to databases containing data obtained from or generated by the use of a product or a related service**.

Database sui generis right, Art. 35

- **'Clarification' of the sui generis right's scope (copyright is unaffected)**
  - Recital 84: 'this Regulation should clarify that the sui generis right **does not apply** to such databases **as the requirements for protection would not be fulfilled**'
  - But: Is this really only a clarification?
- **Background**: **Unclear distinction** between **creation** and **collection** of data in the context of **machine- or sensor-generated data**
  - **Creation** of data **does not qualify as 'substantial investment** in the obtaining, verification or presentation', Art. 7 (1) Database Dir.
  - Underlying rationale: **preventing sole-source situations**
  - **But: in many IoT-situations data will be 'obtained' due to current law**
- **In sum: appropriate solution for this particular problem … with some shortcomings**

Database sui generis right, Art. 35

- **General problems unsolved**
  - **Classic hold-up situations remain unsolved**
    - E.g. in the context of data sharing networks, employment relationships
  - **Access to complete aggregated datasets as a challenge**
    - **In general**: Certain **flexibilisation** in **CJEU CV Latvia vs. Melons** (2021) on screen scraping – but still legal uncertainty
    - **Exceptions and limitations** of the Database Directive **insufficient**
    - **Compulsory licenses** or even **exceptions** for situations where use of the database is indispensable to market entry in related markets or for innovative products/services in a data biotope?
  - **Exception for databases *of* public bodies (g2b)**
  - **Term of protection** – should be shortened to 3yrs max.

Database sui generis right, Art. 35

- **Specific problems unsolved**
  - **Art. 35** of the Data Act attempts to resolve problem of **machine-generated data**
    - **More differentiated solutions would have been possible, but the current version is an acceptable approach**
  - **To make this effective,** a pre-emption clause should be added excluding additional layers of protection in Member States Laws, and
  - The intertemporal application of this **change** should be addressed.
- **Additional need for reform!**

Summary and perspective

- **Data Act attempts an ambitious, sweeping regulation for certain data access case groups in the IoT sector**
- **General concern: Justification for such a broad approach to de-commodify the control of and liberate all aftermarkets in the IoT sector (including B2B)?**
- **→ Concerns in detail:**
  - **Balancing with IP rights as an intricate challenge**
    - Trade secrets
    - Data protection law
  - **Overlap issues**
    - Coherence of the entire 'data package'
    - Contract law and lacking non-mandatory standards for data contracts
  - **Enforcement**, in particular private enforcement

Summary and perspective

- **Database Directive**: **Additional need for reform!**
  - **Art. 35** solves **one particular problem** (i.e. machine-generated data) **in a rather sector specific and unspecified way**
  - But certain **'technical' improvements** will be necessary
  - … and other more **general problems** of the sui generis right remain unsolved

Summary and perspective

Thank you very much for your attention!

Matthias Leistner

https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=2742264