# The EU “Data Act”: A Critical Analysis

**Prof. Dr. Wolfgang Kerber**
(University of Marburg)

Fachausschuss (GRUR) „Recht der Daten“
21 March 2022

# 1. Introduction (1)

**The Data Act proposal: Overview** (published: February 23, 2022)

Three main data governance issues:

(1) Governance of the data generated by IoT devices: (Ch. II)

+ new rights of users of IoT devices to use and share the generated data
+ in B2C and B2B contexts

(2) Business to Government: data access obligations in a public emergency (Ch.V)

(3) Switching between data processing services, solving lock-in problems (Ch. VI)

Additionally:

- General rules if legal obligations for making data available, e.g. on fair, reasonable and non-discriminatory terms (but also reasonable compensation) (Ch.III)
- Fairness of contractual terms in data-sharing („imbalances in negotiation power“) for micro, small- and medium-sized enterprises (Ch. IV)
- Data interoperability (Ch. VIII)
- Non-applicability of the sui generis right for database protection (Directive 1996/9/EC) for sharing IoT data (Ch. X)

# 1. Introduction (2)

**Policy background: Data governance of IoT devices**

- Communication: “Building a European Data Economy“ (2017)
  - \+ data policy for more reuse and sharing of data
  - \+ “data producer right”: exclusive rights on IoT data for owner, long-term user of the IoT device
  - \+ doubts about exclusive rights => start of data access / sharing discussion
- since 2016: controversial open policy discussion about “access to in-vehicle data and resources” (car manufacturers ⇔ independent service providers) with option of reform of sectoral “type approval regulation for motor vehicle”
- generally: competition / consumer choice in aftermarket services (repair etc.)
- parallel discussion about access to agricultural data („smart agriculture“)
- new discussion about data access / sharing in B2B IoT contexts

=> EU data policy has focused primarily on voluntary solutions

- \+ Data Governance Act: data intermediaries
- \+ Digital Markets Act: only very few and specific data access / sharing obligations

=> Data Act was seen as project for defining new data access / sharing rights

# 2. Problems of IoT data governance / objectives of „Data Act“ (1)

**Problems regarding data in IoT contexts:**

- Legal situation: Many generated IoT data are (problem of mixed data sets)
  - + personal data: EU data protection law remains fully applicable (consent)
  - + non-personal data, for which no „de jure“ rights exist, but data holders can have **exclusive de facto control** over the data
- **Main problem: (**both in B2C and B2B contexts)
  - + Manufacturers of smart devices can **get through their own technical design exclusive de facto control** over all data generated by device
  - + **access problems for**:
    - > **users** who (co-)generate the data by using their device
    - > **firms etc.** for providing services but also for data-driven innovation

=> problems:
- competition problems, e.g. on secondary markets
- negative effects on choice of users for services etc.
- negative effects on innovation / under-utilization of data
- no fair sharing of the value of data

# 2. Problems of IoT data governance / objectives of „Data Act“ (2)

Data Act acknowledges this main problem and wants to solve it

**Objectives of the Data Act:** (DA, p.2/3)

In this context, the Commission puts forward the proposed **Data Act** with the **aim of ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data**.

The proposal will help achieve the broader policy goals of ensuring EU businesses across all sectors are in a position to innovate and compete, effectively empowering individuals with respect to their data, and better equipping businesses and public sector bodies with a

**Facilitate access to and the use of data by consumers and businesses, while preserving incentives to invest in ways of generating value through data.** This includes increasing legal certainty around the sharing of data obtained from or generated by the use of products or related services, as well as operationalising rules to ensure fairness in data sharing contracts. The proposal **clarifies** the application of

=> - consumer empowerment and better additional services / competition on secondary markets
- making more data available for firms, for innovation, esp. also for SMEs
- fairness in the allocation of value from data among actors in data economy
- preserving incentives to invest in generating value through data

# 2. Problems of IoT data governance / objectives of „Data Act“ (3)

**Data access and data-sharing rules for users of IoT devices: Overview**

Ch. II: B2C and B2B data sharing

Art. 3: Obligation to make data generated by the use of products or related services accessible

1. Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user.

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

1. Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic

Art. 5: Right to share data with third parties

1. 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, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.

# 3. How does the Data Act change the „rights“ on IoT data? (1)

**„De facto exclusive control“ position of data holders**

- Does the DA change the „rights“ of the manufacturers?
- DA does not change the „de jure“ rights of the manufacturers (rec.5), but acknowledges and justifies the de facto options of manufacturers to use / sell these data
- DA justifies de facto exclusive control of (the use of) the data as an incentive for generating them (=> very close to a traditional IP rationale!)
  + consequence: protecting the position of exclusive control over the IoT data through number of provisions in the DA (see below)
- Important: manufacturer need not be the data holder (position can be „sold“)
- Important result of DA: legal recognition of de facto position of data holder and its economic implications by the legislator as „legitimate“
  (w/o conferring a „right“ to manufacturer or data holders: see recital 5)
  + they already have this („power“) position right now, but so far there were no rules about IoT data => so far unclear whether this is legitimate !

=> Data Act is huge „win“ for de facto holders of non-personal IoT data!

[but: based upon contract with users ! Art. 4 No.6; see later]

# 3. How does the Data Act change the „rights“ on IoT data? (2)

Philipps Universität Marburg

**„Rights“ of other stakeholders**

- **Other firms etc. that would like to use the data**, e.g. for aftermarket services, innovation („third-parties“)
  - \+ DA wants to make IoT data available to them but **no direct access rights** to IoT data (no extension of data access rights)
  - \+ third-parties can get access to these data only via:
    - > request by the user for data sharing (with FRAND conditions) or
    - > buying directly access to the data from data holders
  - \+ [connected cars: service providers want additionally direct access rights]
- **Manufacturer of IoT device**: has **no direct access right** to generated data of its own IoT device, e.g. component supplier in the car (tyre / battery manufacturer)
- **User of the IoT device:** (owns, leases, rents a device)
  - \+ right to access the generated data (but not derived / inferred data)
  - \+ right to request that the data holder shares the data with a third party
  - \+ important: „inalienable“ right (cannot be waived in a contract or sold)

  => „**user“ is the only one who gets an explicit „right“ on data** through DA !

# 4. Data access and sharing rights of users: Analysis (1)

## Art. 3: Obligation to make IoT data accessible

> Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user.

- far-reaching provision about the (technical) design of IoT devices
  - \+ plus transparency about generated data, whether continuously or in real-time, and the identity of the data holder who has to make data available
  - \+ whether the manufacturer supplying the product or the service provider providing the related service intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used;

# 4. Data access and sharing rights of users: Analysis (2)

Philipps Universität Marburg

## Art. 4: Right of users to access and use data generated by IoT device (1)

> Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic

- Looks like a far-reaching right:
  - \+ on a simple request of the user, data holder has to make the data available (w/o need for any further information, e.g., about how it will be used)
  - \+ user seems to be free how to use the data, except
    - > not to compete with data-generating device itself
    - > protecting trade secrets (technical measures), data protection rights
- But: „data access“ / „make data available“ does not imply right of a data transfer
  - \+ (8) The principles of data minimisation and data protection by design and by default are essential when processing involves significant risks to the fundamental rights of individuals. Taking into account the state of the art, all parties to data sharing, including where within scope of this Regulation, should implement technical and organisational measures to protect these rights. Such measures include not only pseudonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allow valuable insights to be derived without the transmission between parties or unnecessary copying of the raw or structured data themselves.

  => only an „in-situ data access right“ (see rec. 21) (data holder can keep control)

# 4. Data access and sharing rights of users: Analysis (3)

Philipps Universität Marburg

## 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, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.

- basic idea: for additional services (e.g. repair), for new services (innovation)

## Art. 6: Obligations of third parties receiving data at the request of the user

> A third party shall process the data made available to it pursuant to Article 5 only for the purposes and under the conditions agreed with the user, and subject to the rights of the data subject insofar as personal data are concerned, and shall delete the data when they are no longer necessary for the agreed purpose.

- Data holder and third-party conclude a („licensing“) contract about data access,
  - \+ in which the user has the right to define through its contract with the third-party the purpose for what the data should be used,
  - \+ requires a negotiation between the data holder and the TP (FRAND with „reasonable compensation“ for making data available, protection of trade secrets etc.) (with dispute settlement mechanism) (Ch. III: Art. 8-10)
- In my view: > this is **not** a data portability right
  > only a right to let others use these data

# 4. Data access and sharing rights of users: Analysis (4)

**Additional rules:**

- Who can be TP? Firms, non-profit organizations, intermediation service provider
  + **but not:** Firms that are **„gatekeepers“ in „Digital Markets Act“**
- (consumer) protection of users against TP: no coercion, deception, and manipulating of user (dark patterns) or profiling the users (Art. 6 2 (a) (b)) etc.
- (but also protection of TP against being monitored by data holder)
- Important: Protection of trade secrets of data holders (through technical measures) plus additional far-reaching protections of economic interests of data holders
  + see Art. 11 (para.2: remedies from the IP toolbox)

**Key question: For what can the data be used? Can they be sold?**

- data can be used for all legal purposes (rec. 28)
- but not for competition with IoT device itself but possible for aftermarket services etc., even if the data holders offer these services
- **Unclear:**
  + Can access to the data be sold to TP?
  + making data available to innovators for money / service?
  + additional supply for data intermediaries and data markets?

# 4. Data access and sharing rights of users: Analysis (5)

**Effectiveness of data sharing mechanism in practice? (1)**

- Key idea: data access to firms through user-initiated data-sharing mechanism
- Experience of ineffectiveness with data portability right (Art. 20 GDPR)
  - + so far DPRs did only work if heavily regulated: PSD2, phone number portability
- Will this mechanism work better than Art. 20?
  - + How much data will be made available? To what extent will it help innovation?
  - + Will it lead to more, better, and cheaper services for the users?
- positive: continuous real-time access plus helping with data interoperability
- Problem group I:
  - + negotiation process between data holder and TP; dispute settlement; How long will it take? Transaction costs?
  - + experience with negotiated FRAND solutions w/o a regulator? What is „reasonable compensation“? Disputes about protection of „trade secrets“?
  - + TP might get only „in-situ access“ to the data: Does this limit the use and value of the data? Costs of using „in-situ access“? (Can SMEs do this?)
  - + what about effectiveness of enforcement?

# 4. Data access and sharing rights of users: Analysis (6)

**Effectiveness of data sharing mechanism in practice? (2)**

Problem group II: To what extent does this data access help?

- Problem 1: it is unclear whether the scope of data that is made available is sufficient for providing additional services or for new innovation
  - + only raw data, and only from individual user: enough for repair service, for predictive maintenance services, for innovation?
  - + also processed / derived data might be needed, or data from many users, and possibility to combine data from different sources
  - + (crucial: that the data can be aggregated/combined/tradable on data markets)
- Problem 2: lacking technical interoperability
  - + for many aftermarket and other services it is necessary to have technical access to the IoT device (requires access to tools and software)
  - + Data Act does not address this at all (only data interoperability)
  - + often necessary: FRAND access to IOT device / software etc.
  - => very unclear how useful these rights are for the users and innovating firms

# 4. Data access and sharing rights of users: Analysis (7)

Philipps Universität Marburg

**Effectiveness of data sharing mechanism? (3): Example connected cars**

- „Extended vehicle“ concept: ensures exclusive control of car manufacturers over
  - \+ access to the generated data
  - \+ technical access to the car (closed system / no interoperability)

=> Gatekeeper position to ecosystem of connected car with control over secondary markets with negative effects on competition, innovation, and consumer choice

- Data Act would give a data sharing right to the users
  - \+ problem 1: raw data are not sufficient for repair service providers etc.
  - \+ problem 2: no technical interoperability
  - => User sharing right of Art. 5 does not solve the problem
- additional sectoral regulation is necessary (update of type approval regulation)
- Question: Is this so different for repair services etc. for other IoT devices?
- Problem: protecting competition / supporting innovation on secondary markets often requires a targeted approach, which Data Act does not offer
- Why not look for other data governance models for connected car that avoid the emergence of such a gatekeeper position? (other options exist … )

# 4. Data access and sharing rights of users: Analysis (8)

Philipps Universität Marburg

**Effectiveness of data sharing mechanism? (4): Conclusions**

- very skeptical whether this leads to an effective mechanism
- unclear to what extent these rights lead to more, better, and cheaper services for users (more competition, innovation and consumer choice)
- low incentives for consumers to use these rights (as data portability right)
  + perhaps better in B2B contexts
- Danger that only few data are made available to innovators with this mechanism (too difficult, too slow, too costly for most firms, esp. SMEs, and easy to obstruct)
- Data sharing mechanism would work better, if
  + clearly regulated regarding scope of data, standardised contracts / processes, where TP can initiate data sharing, effective enforcement by a regulator
  + these user data could be traded and offered on data markets (increases user incentives but endanger data holders‘ exclusive control)

=> serious doubts about entire approach of relying only on such an user-initiated data sharing right for making data available for innovation and competition

# 5. Data holder: Incentives, market and data power (1)

Philipps Universität Marburg

**Do we have an incentive problem regarding IoT data? (1)**

- Summarizing the position of data holders:
  - \+ they get from DA a strong protection of their exclusive control over the IoT data
  - \+ it is not an IP-like absolute right but their commercial use of these data is legally acknowledged, and far-reaching measures for protecting their exclusive control (technical protection, „in-situ access rights“ etc.)
  - \+ due to the weak mechanism of user sharing rights this exclusive control will only be limited to a small extent
  - => they have **de facto an IP-like protection of the data** generated in IoT devices [we come to the contract later]
- DA justifies this with „preserving incentives to invest in ways to generate value through data“ (DA, p.3)
  - \+ classical IP rationale for exclusive rights on a non-rivalrous intangible good
  - \+ classical solution: balancing need for investment with the benefits of broad use this non-rivalrous good (marginal costs of additional use = zero)

# 5. Data holder: Incentives, marekt and data power (2)

**Do we have an incentive problem regarding IoT data? (2)**

- Making the incentive argument here in the DA so strong is entirely surprising
- So far no concerns or any evidence for an underinvestment in IoT devices or in using too few sensors, cameras, microphones in IoT devices
  + everybody predicts a fast exponential spread of IoT devices and the huge increase of collected data through them
  + incentives for data collection have so far not played any prominent role in the discussion about IoT data (also not in the studies for DA)
- Too low incentives will only be a minor or no problem:
  + it is only about the generated data itself, not about inferred/derived data (investments of extracting value from the data are not affected by DA)
  + as owners of the IoT devices the users already have paid a price, which solves incentive problem to invest in generating the data that are important for the functionality of the device for the consumers
- But: danger of over-investment in generating IoT data:
  + manufacturers get large incentives for more sensors to collect additional data not necessary for functionality of IoT device => danger to privacy

# 5. Data holder: Incentives, market and data power (3)

**Data power, monopolistic prices, gatekeeper problems**

- Not discussed in DA: possible negative effects through protecting exclusive de facto control of IoT data by data holders
- Many data sets will be unique and therefore allow monopoly prices: leads to under-utilization of data (P > marginal costs of using them)
- Competition problems: gatekeeper problems in IoT ecosystems with negative effects on secondary markets
- Many manufacturers will „sell“ data-holding position to data companies (free data market), who specialize in commercializing them
  - \+ danger of data concentration with few very large data companies
  - \+ might well be GAFA / gatekeeper firms (DMA)
  - \+ can also lead to additional competition problems
  - \+ users are not allowed to make their data available to gatekeeper firms (as TP) but data holders face no restrictions selling the IoT data to these firms

=> Protection of exclusive de facto control of data can lead also to potentially high additional costs through high data prices, data power and market power (not considered in DA)

# 6. Effects of the Data Act: Intermediate results

**Will the objectives be fulfilled?**

- **consumer empowerment**:
  - + weak mechanism for user rights to access and share IoT data
  - + unclear whether this lead to more, better, and cheaper services
- **Making data available for innovation, esp. SMEs:**
  - + unclear to what extent these rights help other firms, esp. SMEs
  - + presumably only limited amount of data are made available
- **Data collection incentives of manufacturers / data holders**
  - + (very) high incentives through strong protection of exclusive control and weak user rights mechanism
- **Fairness of sharing of value of data**
  - + fairness only addressed B2B with respect to SMEs (negotiation power)
  - + fairness not addressed in B2C situations: very asymmetric distribution of value of IoT data between data holders and consumers

**=> Expected result:** Objectives of Data Act will not be achieved, primarily through too much emphasis on incentives for data collection for data holders

# 7. Neglected key issue: Initial contract with user (1)

**Key role of the contract between manufacturer/seller and user**

- So far not considered: **initial contract** betw. manufacturer and user (sale etc.)
- Art.4

6. The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. The

+ rec. 24:

agreement may be part of the sale, rent or lease agreement relating to the product. Any contractual term in the agreement stipulating that the data holder may use the data generated by the user of a product or related service should be transparent to the user, including as regards the purpose for which the data holder intends to use the data. This

- this implies: the de facto control position over data alone does not give the data holder the right to use any non-personal data without the consent of the user
  - \+ using the data itself or for others, sharing it with others, extract value from data (data analytics) etc. only possible, if agreed upon in contract with the users
  - \+ (i.e. manufacturer / data holder has no direct „rights“ to use the data)

=> theoretically, this looks like a strong position of the users !? Can they use it?

# 7. Neglected key issue: Initial contract with user (2)

**How will these contracts look like?**

- Data Act does not say anything about this but expects clearly a scenario that the users will accept an agreement, in which the manufacturer
  - + will get for the entire „life“ of IoT device („lock-in“ for consumers) the right to use all generated IoT data for all possible uses, sharing / monetizing them (plus right to „sell“ the data holder position to others)
  - + and without directly paying the users for agreeing to this use of the data
  - + (w/o any discussion, DA assumes that the users will agree in the contract to the current solution, where data holders are free to use the data as they wish)
- This is a surprising assumption (because we have a market …)
- In B2B contexts this will be negotiated, and depending on economic conditions (and negotiation power), this can also lead to results that the users will have control over the IoT data (or even become themselves the data holders)

> Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by the data holder. This

  - + acknowledged in DA but only as an exception? (rec. 24)

# 7. Neglected key issue: Initial contract with user (3)

**Market failure problems regarding this contract**

- Very different in B2C contexts: serious market failure problems can be expected
  - + wellknown problems with „consent“ regarding personal data
  - + consumer have information / behavioral problems, do not understand the contracts, value of data etc., and accept everything regarding data
  - + manufacturers do not offer different options / granular choice, but only offer choice of accepting the terms or the IoT device cannot be used
- DA does not address this market failure problem: except transparency, but not coercing, misleading, or manipulating consumers (e.g., „dark patterns“)
- It cannot be expected that competition emerges about the conditions of letting the data holders use the generated IoT data
  (similar to problem of failing competition with privacy-friendly terms)
- Very surprising: neither the DA (nor any of the studies) does even mention this entire issue, i.e. that we have here a market, and whether it works
  - + clear: DA implicitly assumes that this market does not work (B2C and B2B)
- For B2C: DA might be right but what is then the role of this contract?

# 7. Neglected key issue: Initial contract with user (4)

Philipps Universität Marburg

**Conclusions and further policy options**

- Consumer empowerment and fairness:
  - \+ theoretically strong position of consumers through contract does not translate into more consumer empowerment (due to market failure)
  - \+ DA does not expect that contract would give consumers more control over how data holders use their IoT data, or a sharing of value of data (data revenues)
  - \+ contract has no function in that respect (very confusing as market result)
- What can be done for more consumer empowerment?
- For example: giving consumers more choice in contract
  - \+ granular choices what data the data holders are allowed to use for what
  - \+ data holders only collect data necessary for functionality of IoT device, close to idea of „data-avoiding“ products (Maximilian Becker)
  - \+ terminate the contract with data holder and switch to another one, for solving „data holder lock-in“ problem regarding data
  - => these are additional options to „user access and sharing right“ of DA !
- Many other consumer protection measures …

# 8. Other problems and conclusions (1)

Philipps Universität Marburg

**Other problems**

- Horizontal regulation for all IoT devices: might be too ambitious
  - + for B2B and B2C (despite different market failure problems)
  - + horizontal ⇔ sectoral regulation
  - + To what extent will DA pre-empt other governance solutions (also MS level)?
- No comparative analysis of alternative data governance solutions for IoT data
  - + DA: only model with exclusive de facto control of data holder
  - + why not IoT governance models with control over the data by users or by data trustees? (see TRL report 2017 about access to in-vehicle data)
- Many open questions also in B2B contexts, where different problems will emerge,
  - + e.g., through complex relationships in value creation networks with many firms
- Unclear relationship with DGA and DMA
- … what is „reasonable compensation“ in FRAND solution etc.
- Enforcement questions …
- AND: Interplay with data protection law ?

# 8. Other problems and conclusions (2)

Philipps Universität Marburg

**Preliminary conclusions**

- Very good and necessary:
  - + solving problem of exclusive de facto control over IoT data by manufacturers
  - + empowering consumers
  - + making more data available for innovation and competition

  => But: this weak user access and data-sharing right is not sufficient
  => Much more is needed!
- This is a huge, very ambitious, and difficult project about data governance in IoT contexts => will be very controversially discussed
- Deep conflicts of interests about control over data and how to share value of data:
  - + European (large) firms ⇔ US tech firms (= gatekeepers in the DMA)
  - + between firms, partly larger firms ⇔ smaller firms
  - + IoT data-holding firms ⇔ consumers (and public interests)
- many, unclarified questions (regarding legal, technical, economic issues)
  - + important: much research and analysis is necessary before legislators should decide on the Data Act => do not rush to legislation !