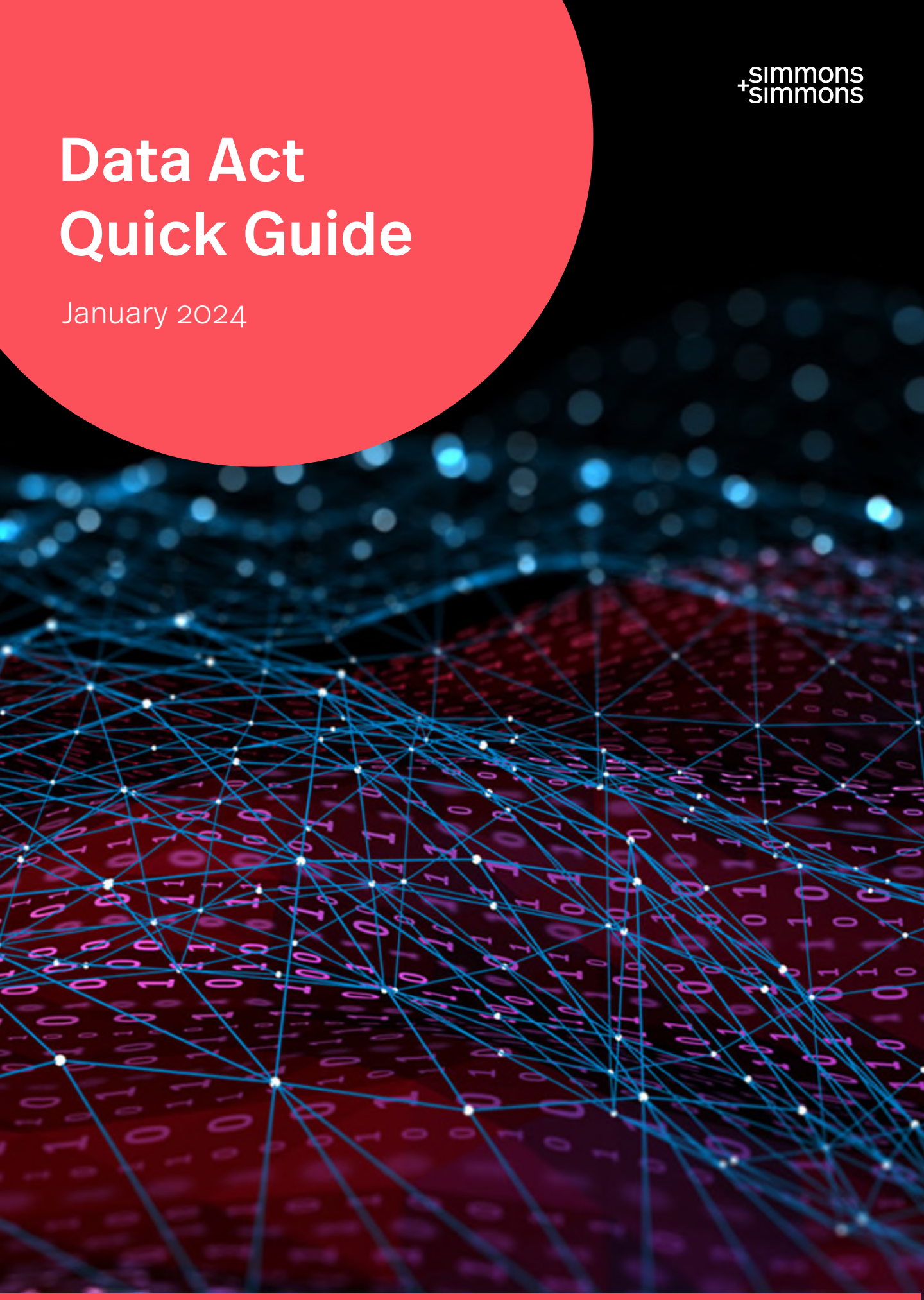
simmons+simmons

Data Act Quick Guide

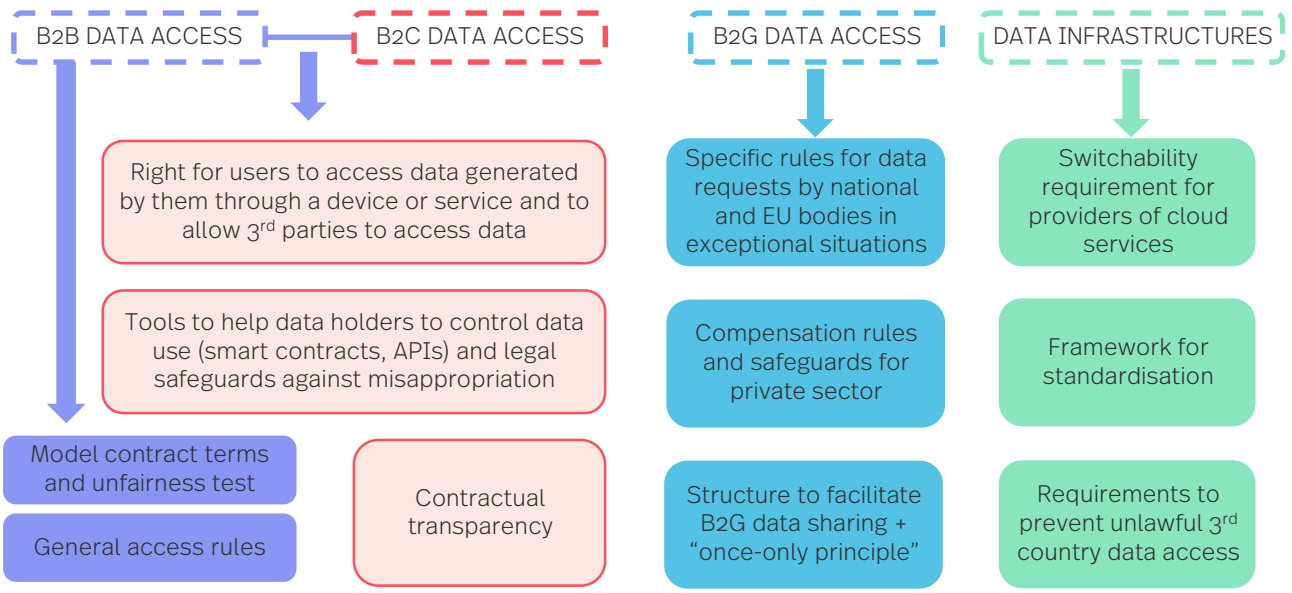
January 2024



What is the EU Data Act?

- The EU Data Act regulates **access to and use of product data generated by connected products or related services** by individuals or companies that own the connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services ("users").
  - This includes data generated by the use of connected products or provision of related services (with or without user interaction) ("product data"). This also includes pre-processed data. In scope is, amongst others, data generated by sensors, data recorded by embedded applications and result or by-product of user's action ("diagnostics data").
  - Not in scope of the EU Data Act: Content itself / data created by user, data transmitted to the connected product for storage purposes (servers / cloud), derivative data (outcome of additional investments), testing of new products.
- The EU Data Act sets out obligations of data holders to **make data available to public sector bodies and EU institutions, agencies or bodies** based on "exceptional need".
- The EU Data Act regulates **switching between cloud service providers** that process data. Since such a requirement means that existing data processing services must be compatible with each other, the EU Data Act finally regulates requirements for the interoperability of data.

Schematic Overview



Timeline

- The EU Data Act entered into force on **11 January 2024.**
- The EU Data Act act will generally become applicable **as of 12 September 2025**.
- The obligation to make connected products and related services data readily available to the user applies as of 12 September 2026.

B2B / B2C Data Access: What is in scope?

Connected products

An item that:

- obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, **and**
- whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user."

Related services

Digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that:

- its absence would prevent the connected 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 connected product"

- IoT
- incl. vehicles, **industrial machinery**, **medical and health devices**, consumer goods

- linked to operation of product
- incl. services offered by a third party, if supplied under the product's sales, rental or lease contract with user. In case of doubt: in-scope

Extraterritorial Effect

Manufacturer / Provider / Data Holder in country **outside of EU in scope of EU Data Act if they market connected products / related services in the EU**

B2B and B2C Data Access: Key obligations & rights

Key obligations for Manufacturers of Connected Products / Providers of Related Services

Information obligations

Prior to conclusion of agreement (purchase/rent/lease) re product or related service:

User to be informed of:

- nature and volume of data to be generated
- how to access the data
- identity of data holder, including contact details of data holder
- how user may request data sharing with 3rd parties

Design of products / services

To be *designed*, *manufactured*, *provided* in such a way that user is enabled to **easily and directly access data -- including relevant metadata necessary to interpret and use those data (in a common format)**.

Examples:

- user accounts for every user
- access upon simple request mechanisms granting *automatic* execution (not requiring clearance by manufact./data holder!)
- direct access to stored data (on product/3rd party server) ➔ API

Key obligations for Data Holders

Provide User access to product data

- **access**: without undue delay, free of charge and, where applicably, continuously and in real-time
- **data sets**: comprehensive, structured, commonly used & machine-readable format
- **data quality**: same quality as is available to data holder

User: free to use data for any (lawful) purpose, incl.

- Right to share data with 3rd party ("Data Recipient") that offers an aftermarket service
- Service may be in competition with a service provided by Data Holder

UPON USER REQUEST:

Provide Data Recipient with (direct) access to data

Same requirements as towards User (left box) apply

- May use for **aftermarket service**, **even if** in competition with Data Holder's services!
- **Certain use restrictions**, e.g. shall not
  - Use for other purposes than agreed & received
  - pass on to another third party and/or "Gatekeeper" (DMA!)
  - Use data to develop competing connected product

Data Recipient:

- A natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available.
- Including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law

Data Holder:

- De facto control of data
- May be, for example,
  - Manufacturer
  - Provider of related services
  - External cloud storage provider (e.g. if cloud storage is integral to the product) (Recital 22)
- Multiple data holders in relation to generated data possible

B2B and B2C Data Access: further relevant topics

Data Holder – Data Recipient: License

Data Holder required to conclude License Agreement with Data Recipient

- Monetisation of data possible in B2B context!
- Requirement for compensation: Fair, reasonable and non-discriminatory (FRAND) and may include a margin!

Take into account:

- Data format & volume, nature, supply of and demand for data
- Basis for calculation to be disclosed

Trade secrets

Generally:

- **No right to refuse data access based on trade secrets!**

Exceptions:

- **"Serious economic damage"** is highly likely to result from disclosure of trade secrets
- Envisaged **data transfers to third countries** have **weaker** trade secret / confidentiality protections / lack of enforceability
- **Competitors exploit** access to data to reverse-engineer services or devices
- **Refusal** to grant data access by data holder **can be challenged** at court / dispute settlement body

Personal Data

Personal data may only be shared in accordance with GDPR

B2G Data Access: In a nutshell

Data holder to make data available to a public sector body, EU institution etc:

- Upon request by a public sector body in case of "exceptional need", including:
  - Public emergency
  - Prevention of or recovery from public emergency
  - To fulfil a specific task in the public interest (if data cannot be obtained by alternative means or if provision of data significantly reduces burden for other data holders)
- Data holders to provide data free of charge in case of a public emergency
- Compensation for other exceptional need requests: technical and organisational costs (including costs of pseudonymisation/ anonymisation for personal data), plus "reasonable margin"

Reaction deadline:

- **5 days in case of public emergency**
- **15 days for other exceptional need requests**

"**Data holder**" means a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data.

Right to reject data access request made by public sector body

Data Holder may decline or demand modification of request, if:

- Requested data unavailable
- Request does not meet certain conditions:
  - demonstrate exceptional need; state legal basis;
  - be proportionate in terms of granularity and volume of data requested;
  - respect trade secrets, cost & efforts required on the part of the data holder;
  - provide information on penalties for non-compliance (etc.)
- **In case of public emergency, once-only principle applies: data holder may refuse access if it has already provided the requested data to another public institution**

Switching cloud & on-prem data processors

Removing obstacles to effective switching

- Prohibition to impose certain "pre-commercial, commercial, technical, contractual and organisational" obstacles that make switching providers for customers difficult
- Obligations on providers and obligation to include key provisions in contracts, such as:
  - accept **notice period to initiate switching of provider of no more than 2 months**
  - gradually **reduce switching charges** in the years following entry into force of the Data Act
  - provide reasonable assistance to the customer for switching
  - make **open interfaces** publicly available free of charge
  - **export all data (co-)generated**, *including the relevant data formats and data structures*, in a structured, commonly used and machine-readable format
  - provide safeguards for international data flows

Cloud & International Data Flows

Safeguards for **non-personal** data

Providers of data processing services

prevent (as far as possible) **any international data transfer** or governmental access, **where this would create a conflict with EU or member state law**

Third-country judgments ordering transfer or access

only recognised if mutual legal assistance treaty in place or if decision based on rule of law principles

(guidance to be provided by the "European Data Innovation Board" pursuant to 29 DGA)

In case a third-country judgment is recognised

addressees to provide the minimum amount of data permissible

Data holders to be informed of any third-country transfer or access request

prior to complying with request

except insofar as request serves law enforcement purposes

Why companies need to consider this now

Manufacturer / Data Holder

- Implement design requirements in time (Manufacturer / Provider)
- Get to know your data
- Start developing price book for data
- Classify non-personal – personal data (tricky in large data sets / machine data)
- Draft proper data license terms
- Take into account FRAND as far as pricing is concerned
- Prepare for B2G data access requests

Data Recipient

- Assess where / whether your company may profit as Data Recipient (aftermarket services!)
- Negotiate proper data license agreement

User

- Assess where your company may profit from access to data
- Check whether you wish to involve a third-party as data recipient
- Put in place proper agreement with data recipient

Cloud Provider / Cloud Switching

- Structure contracts appropriately
- Be aware of international data flows and interoperability requirements

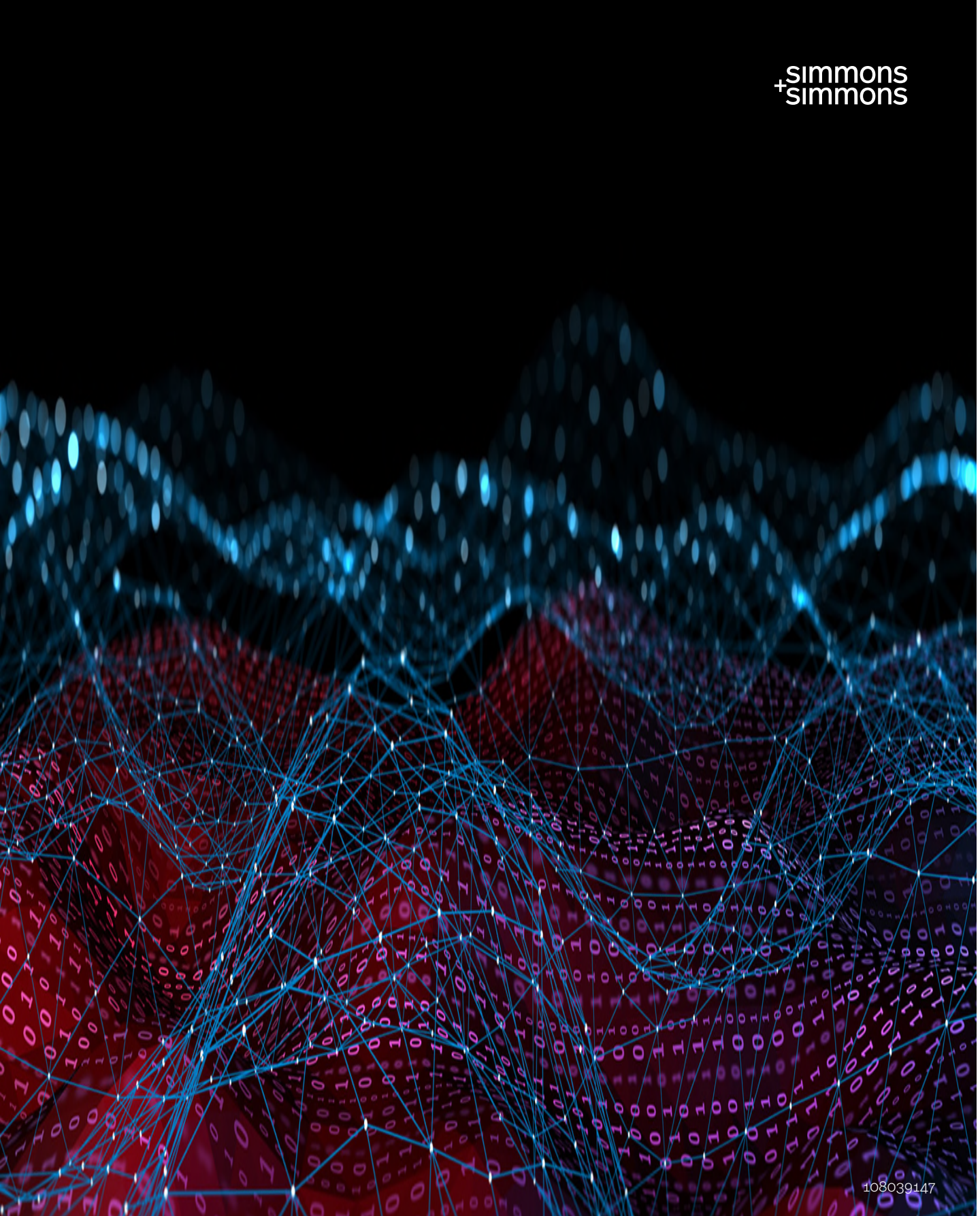
Questions? Please contact:

Christopher Götz, LL.M
Partner
Digital Business
Munich

E christopher.goetz@simmons-simmons.com

- **Watch out for interoperability standardisation being published by the Commission regarding data spaces, cloud services, smart contracts applications**
- **Watch out for member state legislation regarding penalties for non-compliance with Data Act**
- **Enforcement: Each EU member state to designate authority / sanctions**

simmons+simmons



simmons-simmons.com