Deloitte.

CENTRE *for*
REGULATORY
STRATEGY
EMEA

Business-to-Business data sharing under the EU Data Act

Delivering to the regulatory requirement to share data in a fair, reasonable and non-discriminatory manner

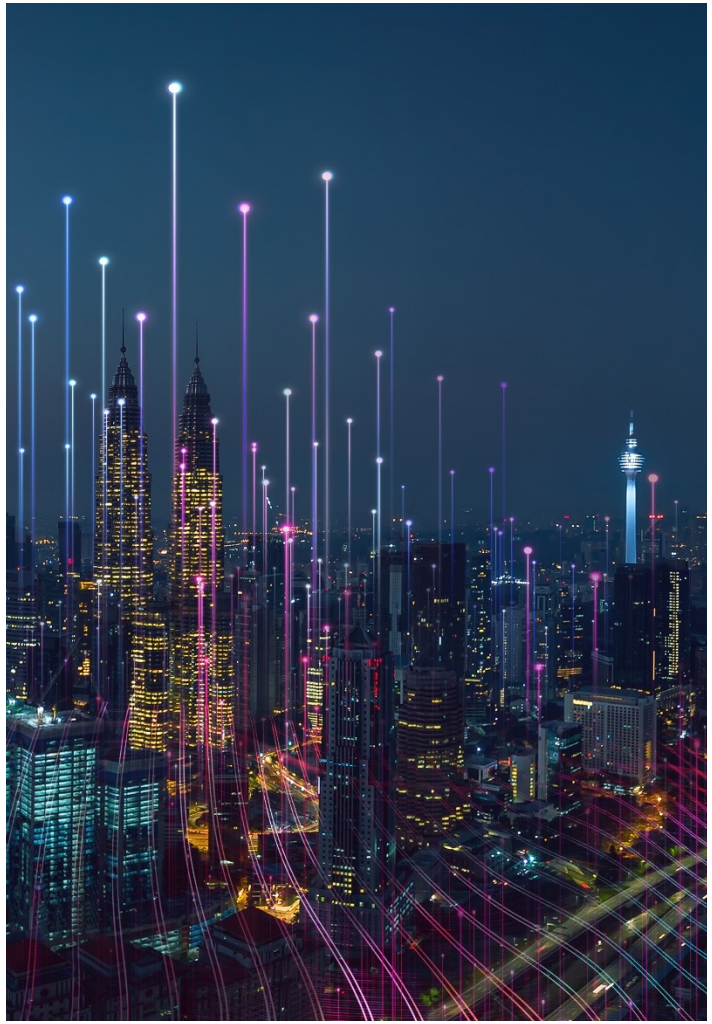
April 2024

MAKING AN IMPACT THAT MATTERS since 1845

Contents

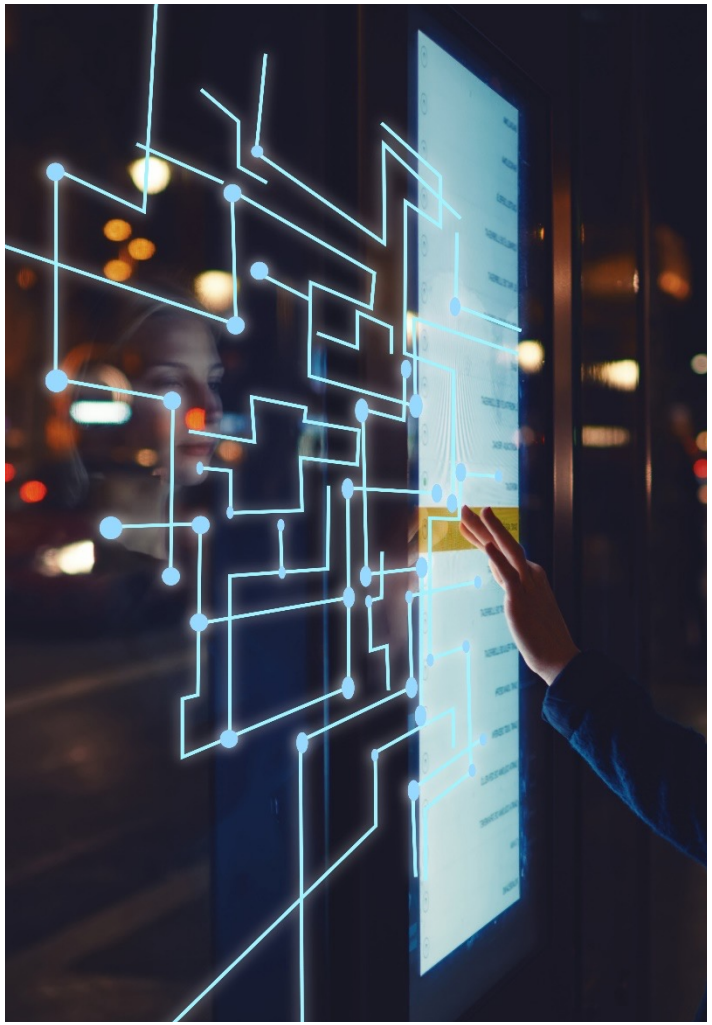
Executive Summary

- The EU Data Act was published in the EU Official Journal on 22 December 2023 and is now in force. It will become applicable on 12 September 2025.
- Under the Data Act, connected products have to be designed and manufactured in a way that empowers EU users (businesses or consumers) to easily and securely access, use and share the generated data.
- It has been estimated that in 2028, the economic impact of the Data Act could imply an increase in GDP of €273 billion (representing an additional 1.98% of GDP).
- To help realise this opportunity, the Data Act intends to create new markets for Business-to-Business (**B2B**) data, underpinned by a new regulatory regime.
- This regime requires business data holders to share data with other businesses on a fair, reasonable & non-discriminatory (**FRND**) basis. Data holders may include a margin when sharing data to businesses other than SMEs.
- The application of FRND obligations to data is novel. However, comparisons can also be made with experiences in other regulated sectors, for example electronic communications and financial services.
- The framework outlined in this document is intended to provide a helpful frame of reference for both business data holders and recipients who may be considering data sharing under the Data Act, on a FRND basis.
- Data Sharing *c*ase studies are included relevant to the health, mobility and agriculture sectors, to highlight key Data Act considerations relevant to each. These sectors are all priority EU Data Spaces.
- This document concludes by outlining the strategic considerations that data holders should consider relevant to commercial data sharing, as well as key steps that can be taken now in order to prepare for Data Act compliance.



Introduction

This document's purpose and intended audience



A key element of the Data Act requires that B2B data be shared with third parties in a FRND and transparent way.

The Data Act is designed to ensure that:

- users of a connected product or related service in the EU can access, in a timely manner, the data generated by the use of that connected product or related service; and
- that those users can use the data, including by sharing them with third parties of their choice.

It imposes the obligation on data holders to make data available to users and third parties of the user's choice in certain circumstances. It also ensures that data holders make data available to data recipients in the Union under FRND terms and conditions and in a transparent manner. The Data Act complements and is without prejudice to EU law on the protection of personal data and privacy.

The purpose of this document is to set out a practical framework that can be used as a starting point by data holders and data recipients to reach agreement on the value of data in a B2B sharing context, consistent with the regulatory obligations in the Data Act.

This document is aimed at the wide range of companies that could be affected by the new B2B data sharing obligations in the EU Data Act

From a **data holder's perspective,** it should be relevant to companies across all sectors of the economy who may receive requests for B2B data under these new rules.

These new rules raise significant strategic and operational implications for data holders, in terms of the strategic decisions around people, processes, systems, pricing and governance that will need to be made.

From a **data recipient's perspective**, this framework should be of particular interest to those companies who may seek to take advantage of these data sharing provisions.

This includes the data intermediation service providers who are expected to facilitate a data economy by establishing commercial relationships between the key players across the data sharing ecosystem.

Introduction

Summary of key provisions – what the Data Act requires in relation to B2B Data Sharing

Article	Issue	Key Provisions
Article 5	Data sharing on user's request	**Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data,** as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time: • Article 5(3) is clear that any company designated as a gatekeeper under the Digital Markets Act cannot benefit from the B2B data sharing provisions (with Recital 40 explaining that such access is not required "given the unrivalled ability of those undertakings to acquire data").
Article 8	B2B data sharing	**Conditions under which data holders make data available to data recipients**: • Article 8(1) – In a B2B context, data holders must make data available to data recipient under FRND terms and in transparent manner; and • Article 8(3) - A data holder shall not discriminate with respect to the modalities of making data available between comparable categories of data recipients, including partner enterprises or linked enterprises. • Therefore Article 8 envisages the possibility of the need to agree non-price conditions relevant to data sharing, in addition to compensation.
Article 9	Further detail on compensation for B2B data sharing	• Data Sharing B2B compensation shall be non-discriminatory and reasonable and may include a margin; • Data holder/data recipient shall take into account: – Costs for making data available (e.g. for formatting, dissemination and storage); – Investment in the collection & production of data, taking into account whether other parties contributed; and – The volume, format and nature of the data. • Micro, Small or Medium enterprises – and non-profit organisations – should only pay a cost-based charge. Article 9 also confirms that the European Commission shall adopt guidelines on the calculation of reasonable compensation, having taken into account the opinion of the European Data Innovation Board.
Article 10	Dispute resolution bodies	Also includes provisions relevant to the **establishment of dispute resolution bodies** who will settle any resulting disputes where the data holder and the data recipient have been unable to agree.

Introduction

The EU Strategy for Data, EU Data Spaces & Member State Data Act implementation case study

EU Data Spaces

The European strategy for data aims to create a single market for data in which data will be able to flow seamlessly across borders and sectors in a safe and secure manner, in line with EU rules and values, for the benefit of European businesses and citizens.

Common European Data Spaces are designed to enhance the development of new data-driven products and services in the EU, forming the core tissue of an interconnected and competitive European data economy.

On 24 January 2024 the European Commission published a Staff Working Document which provides an overview of the status of the common European data spaces.

Data Spaces are currently being developed across the following 14 sectors/domains:

- Agriculture
- Cultural Heritage
- Energy
- Finance
- Green Deal
- Health
- Language
- Manufacturing
- Media
- Mobility
- Public Administration
- Research & Innovation
- Skills
- Tourism

The obligations in the Data Act apply to the whole of the economy and are therefore broader than the EU Data Spaces. However, the EU data strategy envisions strong synergies between the Data Act and EU Data Spaces, which are expected to mutually reinforce each other.

Data Act Case Study: Member State Implementation in the Netherlands

On 4 March 2024 the Dutch government opened a public consultation on a draft Implementation Act for the Data Act. Under the proposed regime:

- The Netherlands Authority for Consumers and Markets will be appointed as the competent supervisory authority and data coordinator in the Netherlands.
- The Autoriteit Persoonsgegevens (Dutch Data Protection Authority) will offer support as a co-supervisor for what concerns data sharing with public sector bodies.

In case of non-compliance, the two authorities will be able to impose:

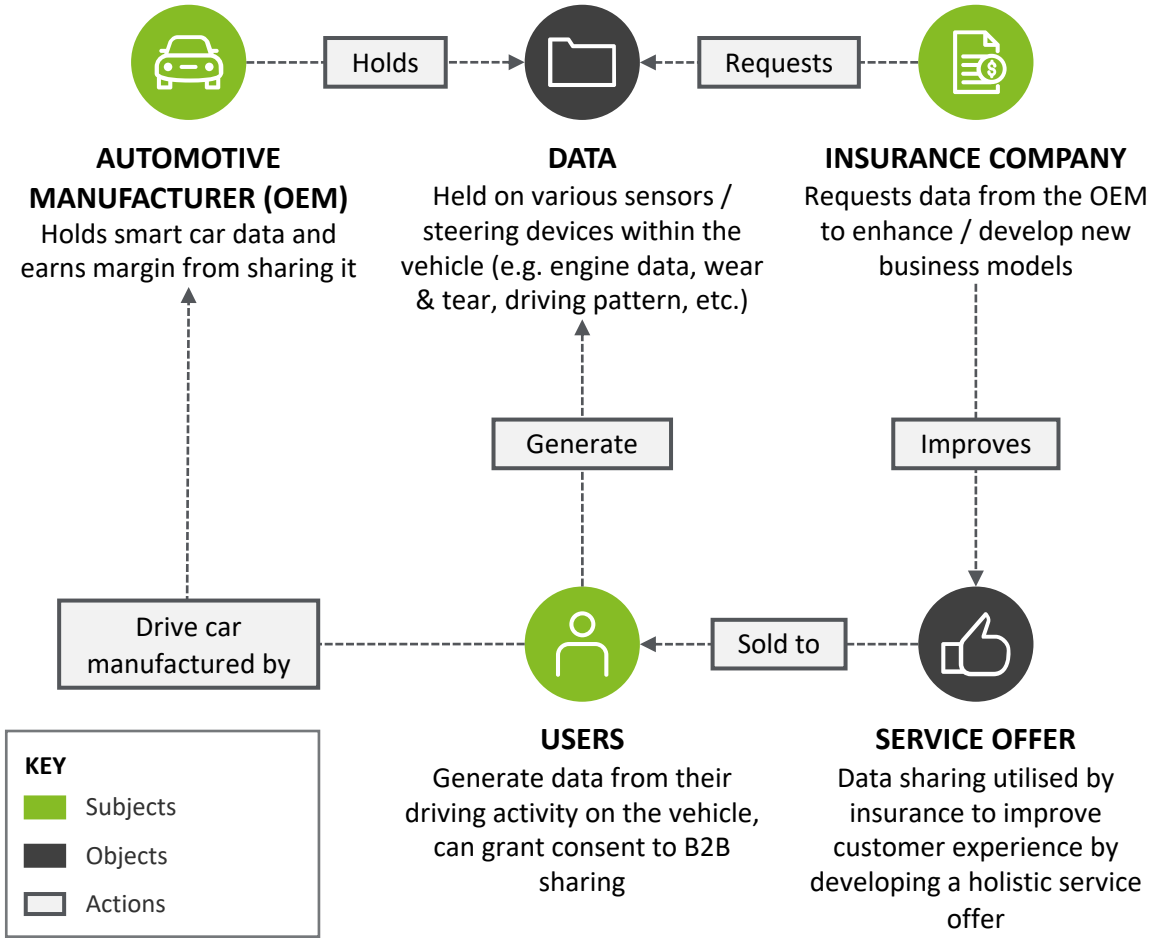
- A binding order; or
- An administrative fine up to EUR 1.030.000 or 10% of the annual revenue (whichever highest).

The Implementation Act amends a set of local rules and is planned to enter into force starting from 12 September 2025.

Sector case studies

Mobility

Automotive Data Sharing



Key Considerations

Data Holder: Automotive manufacturer (OEM).

Data Recipient: Financial services firm / Insurance company seeking to develop new or optimize existing business models.

Case study specific-factors:

- Insurance companies can use the newly acquired data to optimize their risk calculations / estimations and ultimately enhance policies or offer tailored products.
- Other participants on the data market (e.g. online retailers or evaluation platforms) are likely to demand the data as well since they could leverage on the huge amount of technical information as add-on to their data treasure.
- Automobile Clubs or technical service companies could use the data to enhance or tailor their technical services (e.g. model-specific support).

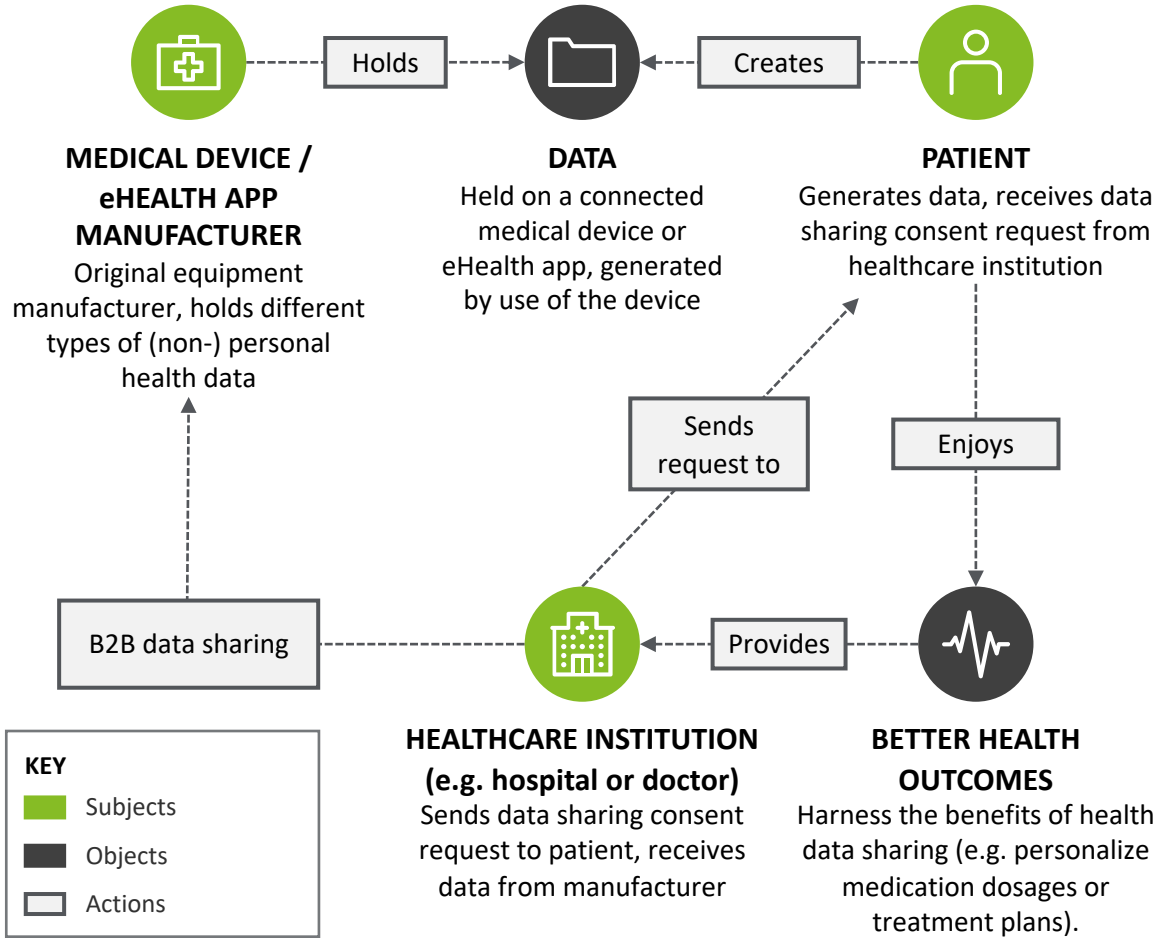
Potential Questions

- Which (technical) data is useful for developing new products and offers?
- How is a reasonable price being determined for the different data types demanded by the recipient (and subsequently for other recipients on the data market)?
- How can sharing be automated and interoperability ensured?

Sector case studies

Health

Health Data Sharing



Key Considerations

Data Holder: Medical device or eHealth app manufacturers, holds different types of (non-) personal health data.

Data Recipient: receives data from the data holder, if user has consented. Thus, the recipient is able to personalize its (healthcare) services towards the user.

Case study specific-factors:

- The Data Act is a horizontal instrument envisaging basic rules for all sectors for the use of data, but also leaves room for vertical legislation to set more detailed rules for the achievement of sector-specific regulatory objectives, especially in the healthcare sector.
- Recital 14 of Data Act explicitly states that it is applicable to medical devices.
- As data holders will possibly face additional costs to make the data available, “reasonable compensation” must be agreed upon for the B2B data sharing processes, considering data volume, format and nature. Small/medium enterprises are granted specific exemptions for this compensation.

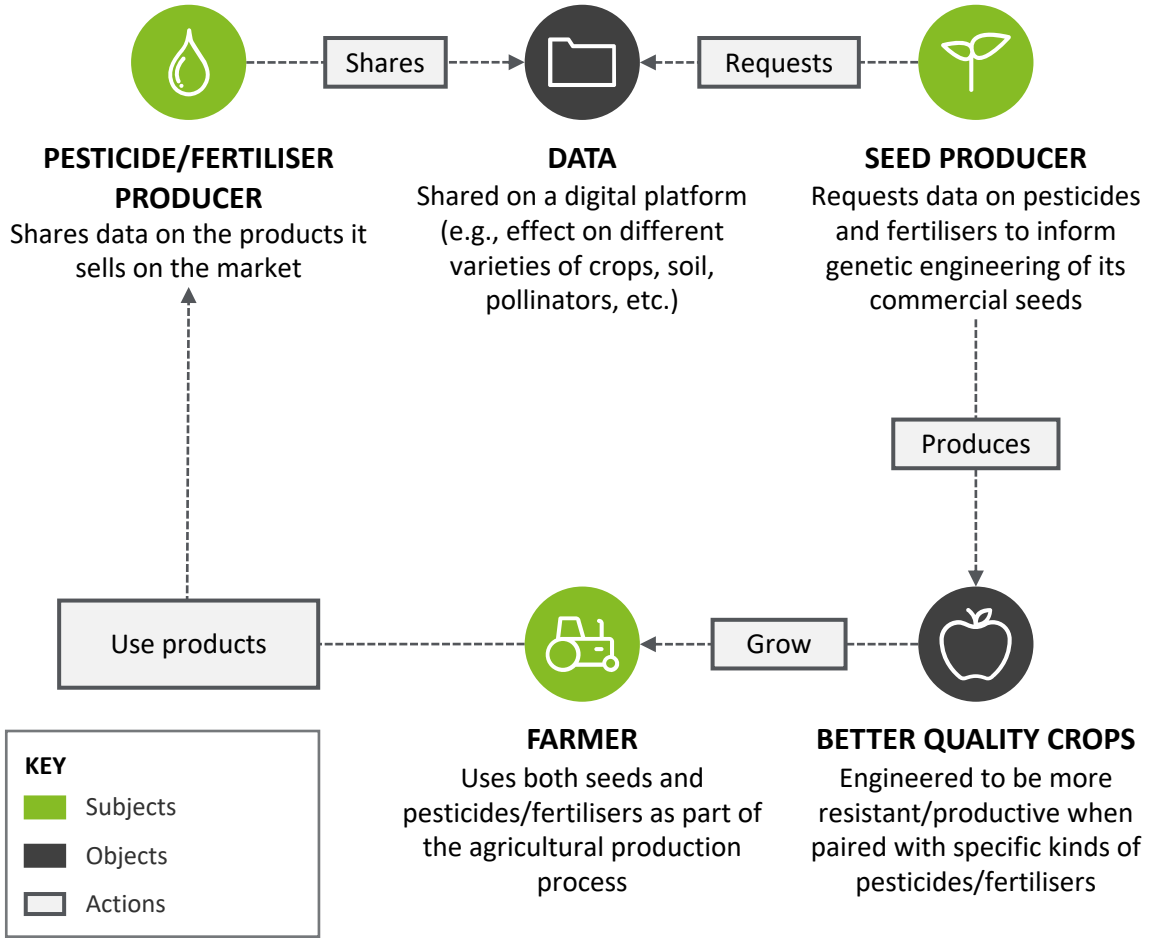
Potential Questions

- Which kind of data will fall within the scope of the Data Act in the context of medical devices and eHealth apps?
- Which additional costs will the data holder face to make the data available (“reasonable compensation” must be agreed upon for B2B data sharing)?
- Interaction with other legislation (e.g. Medical Devices Regulation, GDPR).

Sector case studies

Agriculture

Agriculture Data Sharing



Key Considerations

Data Holder: Pesticide/fertiliser producer.

Data Recipient: Seed producer.

Case study specific-factors:

- The seed producer would be able to use information about specific products developed by the data holder to enhance its plants when paired with that specific product. This in turn would also benefit the pesticide/fertiliser producer by creating 'tailored' markets around its products.
- Data holders and recipients should be mindful of the role of third-parties in the data sharing process (e.g., farmers providing data on yields after using specific combinations of chemical products and seeds).
- Product-efficient seeds could also facilitate compliance with other sectoral regulations (e.g., helping to avoid excessive use of pesticides).

Potential Questions

- Data holders may not be as willing to share product-specific data, as the boundary with trade secrets may be quite blurred. This could be especially relevant if the seed producer belongs to a larger corporate group which also competes in the pesticide/fertiliser market.
- How best to establish transparency, trust and appropriate remuneration with the different players relevant to this data sharing arrangement?

Key considerations relevant to Business-to-Business data sharing

Thinking about the value of B2B data

A key driver for the Data Act is that the full value of data in the European economy is not being realised due to factors such as a lack of clarity regarding who can use and access data generated by connected products.

*It has been estimated that that in 2028, the economic impact of the Data Act could imply an increase in GDP of €273 billion (representing an additional 1.98% of GDP).**

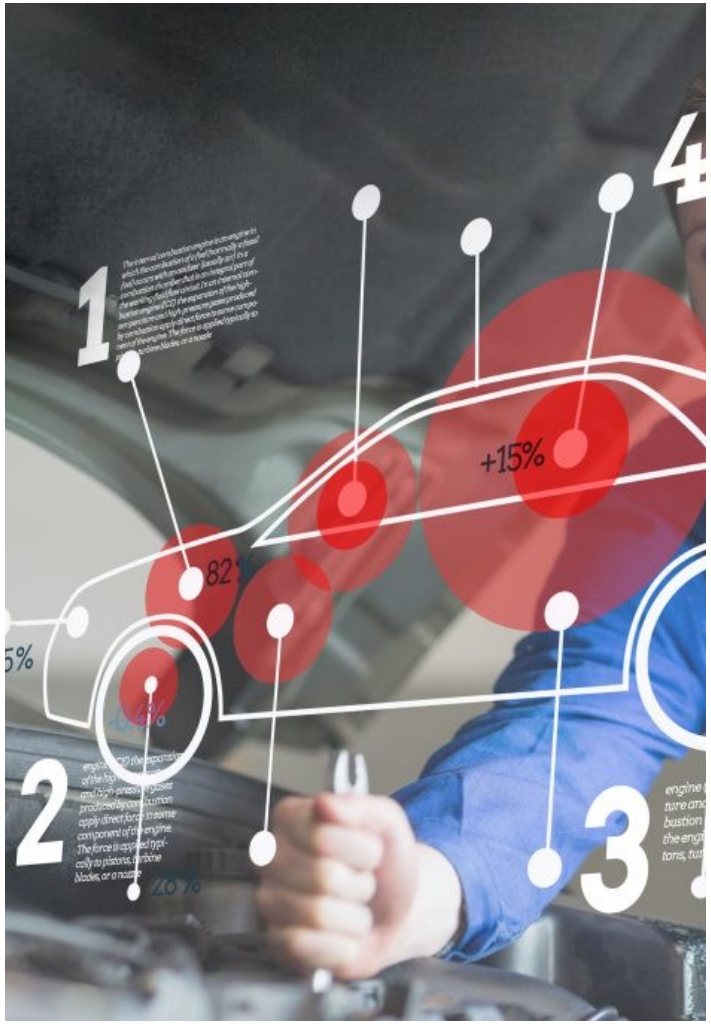
The Data Act has therefore been designed to remove barriers to access data, while preserving incentives to invest in data generation. It is intended to unlock the value of data generated by connected objects in the EU.

There will, of course, be many different commercial scenarios that will be relevant to the provisions of the data, which apply across all sectors of the economy. As has been noted**:

"despite the broad recognition of its value, and the need to develop appropriate policy frameworks, there is still no consensus method for empirically determining the value of data"

"when they are available, market prices are always a preferred method for valuation"

Therefore, this document sets out a principles-based approach to aid parties in their commercial discussions regarding the application of the Data Act provisions which require that such data sharing occurs in a FRND and transparent way.



* Study to support an Impact Assessment on enhancing the use of data in Europe available at Impact Assessment report and support studies accompanying the Proposal for a Data Act | Shaping Europe's digital future (europa.eu)

**'What is the value of data? A review of empirical methods', Diane Coyle & Annabel Manley, Bennett Institute for Public Policy, University of Cambridge, July 2022

Key considerations relevant to Business-to-Business data sharing

Comparisons with electronic communications and financial services regulation

Electronic communications regulation

A commonly used intervention has been the obligation for a provider's services to be offered to third parties in a FRND manner, as part of a regime overseen by the national regulatory authority, with a dispute resolution backstop. Guidance has typically been provided by the regulatory authority on how this requirement should apply in practice.

Companies subject to these obligations have, amongst other things, identified the teams across commercial, technical and legal disciplines responsible for negotiating with third parties, developing the relevant pricing materials, the technical processes and managing the dispute resolution processes.

Financial services regulation

Considerations seen as relevant by the regulatory body (in this example relevant to the granting of access to and licences to use benchmarks on a FRND basis), have included:

- the degree of competition and potential competition in the market;
- whether the aggregate of the fees charged to users bears a reasonable relationship to the costs and risks of producing the specified benchmark, including a reasonable return on capital; and
- whether a provider applies dissimilar conditions to equivalent transactions with relevant users or different categories of relevant users, thereby placing them at a competitive disadvantage.

An initial high-level comparison of both approaches with the B2B Data Sharing obligations in the Data Act

- The data sharing obligation in the Data Act applies to all data holders, not just data holders who may hold a strong market position based on an economic assessment of the provision of a particular service. In the electronic communications and financial services sectors, specific intervention is typically premised on a case-specific competition analysis.
- Similar to telecoms markets, the marginal cost of providing data is likely to be exceptionally small. The majority of costs are likely to be common to all users on a platform.
- The ability of suppliers to obtain a reasonable margin is, generally speaking, a common element across all regimes. It is noted that the Data Act also requires a cost-based charge where the data recipient is an SME or non-profit organisation. Setting a cost-based charge in electronic communications markets is a more onerous intervention (e.g. where the regulator sets a price control).
- Charging different prices between different types of customer (e.g., those in different industry sectors) is typically permitted across all regimes, in the interests of economic efficiency. This is consistent with the requirements of the Data Act which refer to no discrimination between 'comparable categories of data recipient'.
- The Data Act envisages that intervention will not be necessary in the case of 'data sharing between large companies' as they are considered capable of negotiating FRND prices. This observation is at odds with, for example, experience of the frequent need for dispute resolution in the electronic communications sector.

Key considerations relevant to Business-to-Business data sharing

Principles relevant to determining ‘fair and reasonable’ compensation

Principle*	Explanation	B2B data sharing considerations
Cost causation	Costs should be recovered from those parties whose actions cause the costs to be incurred at the margin.	This principle is consistent with the examples of cost recovery already provided for in the Data Act, e.g. costs necessary for the formatting & dissemination of data. However, the incremental costs associated with these elements are likely to be very small. Therefore, a key consideration will likely be how the pricing strategy reflects the allocation of common costs relevant to the data holder’s activities.
Cost minimisation	The mechanism for cost recovery should ensure that there are stronger incentives to minimise costs.	For SMEs and not-for-profit data recipients (where there is a cost-based obligation) this principle is likely to be already built in. Also, the onus on Data Holders to (broadly speaking) bear the costs of dispute resolution would also seem consistent with this objective.
Distribution of benefits	Costs should reflect benefits received.	Art 9(1) of the Data Act is clear that compensation ‘may include a margin’. How much the data recipient is willing to pay for the data is likely to be an important consideration here.
Effect on competition	The mechanism for cost recovery should not undermine or weaken the pressures for effective competition.	This should be a central element of any B2B charging structure, given concerns about ‘gatekeepers**’ using their position to negatively impact competition in the market.
Reciprocity	Where services are provided reciprocally, charges should also be reciprocal.	This is unlikely to be a relevant consideration, given that the focus of the regulation is to facilitate the bidirectional sharing of data in circumstances where it has previously not been shared (i.e. the regulation assumes a data asymmetry between the parties).
Practicability	The mechanism for cost recovery needs to be practicable and relatively easy to implement.	Given the high number of potential requests that data holders may receive, this is likely to be a key consideration.

*These principles (commonly referred to as ‘Cost Recovery Principles’ have been established by Ofcom in the context of its interpretation of ’ fair and reasonable’ pricing in relation to electronic communications services.

** Under the DMA, the European Commission can designate digital platforms as ‘gatekeepers' if they provide an important gateway between businesses and consumers in relation to ‘specified core platform services’ such as browsers or operating systems.

12

Key considerations relevant to Business-to-Business data sharing

Principles relevant to determining ‘non-discriminatory’ compensation

Principle	Explanation	B2B data sharing considerations
Differentiation	Non-discrimination does not mean all users need to be charged the same price.	This is already reflected to some extent by Article 8(3) of the Data Act which highlights the requirement not to discriminate between ‘comparable’ data recipients (see below). But it is worth highlighting this point explicitly – it is not necessarily economically efficient for all data recipients to be charged the same price.
Comparability	That the approach provides a sound basis for ensuring that comparable users are not unduly discriminated against.	A maxim that ‘comparable data recipients should be charged comparable prices for comparable data purchased at broadly similar times’ could be a useful one for data holders to adopt.
Competition (intra-category)	Approach does not distort competition between different users within the same category.	Competition concerns are more likely to arise where there is differentiation between data recipients within the same industry category (e.g. data recipients within the same industry category, such as automotive customers).
Competition (inter-category)	Approach does not distort competition between users in different categories.	Competition concerns are less likely to arise where there is differentiation between data recipients in different industry categories (e.g. between automotive and agricultural sectors).
Maximisation	Pricing maximises total number of users overall.	Pricing strategies should maximise overall usage of the data holders’ B2B data sharing platform. For example, charging all users the same price may deter new data entrants. This principle is already reflected in the requirement to charge SMEs and not-for profit data recipients a cost-based charge.
Practicability	The concept of discrimination can be complex to enforce, the approach should be proportionate.	Recital 32 of the Data Act (introduced late in the negotiation) makes reference to the relevance of the principles of EU competition law in defining the relevant product market. This guidance is clearly sound, however market definition in a competition law context is typically time consuming (in terms of years, not months) and complex. Adopting a similar standard could risk compromising the Data Act’s vision of ‘liquid and efficient’ data sharing across the economy.

Key considerations relevant to Business-to-Business data sharing

Measures relevant to ensuring ‘transparent’ sharing

Measure	Explanation	B2B data sharing considerations
Charging Methodology	A charging methodology would set out the basis on which data holders would calculate FRND charges.	A data sharing charging methodology could be an important step to ensure transparency, consistent with Recital 51 which states that data holder should provide to the data recipient sufficiently detailed information for the calculation of the compensation.
Ratecard	A ratecard could set out the indicative charges that would form the basis for commercial negotiations.	The data sharing ratecard could identify the different ‘indicative’ prices that the Data Holder would intend to charge Data Recipients under the FRND obligation. Such an approach would also help ensure terms are not perceived as ‘unilateral’ and unfair, consistent with the objectives of Chapter IV. This transparency could expedite commercial negotiations with data recipients.
Organisational Structure	In regulated sectors, compliance with a regulatory obligation is aided by a comparably transparent organisational structure (e.g. a distinct ‘regulated’ entity). This type of obligation can be imposed by a regulator (e.g. a requirement for accounting separation or even ‘functional separation’ of wholesale and retail activities).	Although requirements of this type are typically only imposed in markets where competition cannot deliver the expected smooth operation of the market, the fact that the Data Act has not been premised on competition grounds warrants consideration of this type of transparency mechanism. Given the likely costs involved, it would be more suited to much larger companies who occupy a strong market position and will field significant requests for data, for example those companies that have been designated as ‘gatekeepers’ under the Digital Markets Act.
Dispute resolution	Ensuring transparency of dispute resolution processes and outcomes is a key element of ensuring an effectively functioning regime for FRND service provision.	Article 10(10)a of the Data Act requires that dispute resolution bodies make publicly available annual reports on their activities, including the most common reasons for disputes and recommendations on how such problems could be avoided or resolved. This is positive. Given the potential complexities associated with dispute resolution in this area (likely requiring specialist input), parties will eagerly await the identity of the dispute resolution body.

Key considerations relevant to Business-to-Business data sharing

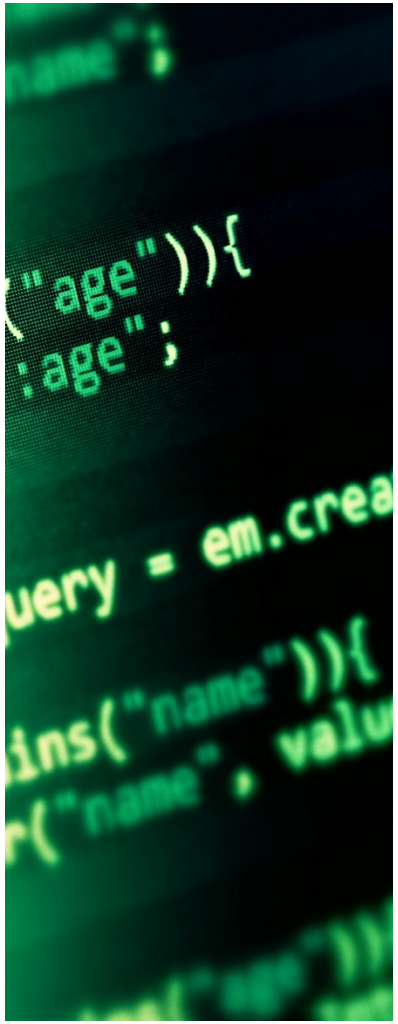
Potential non-price issues that could also be relevant

Issue	Explanation	B2B data sharing considerations
Timescales	The time taken for discussions to conclude is likely to be a key consideration in whether the data holder has acted reasonably or not (i.e. whether it is unduly delaying to make the data available).	Recital 47 to the Data Act states that "Long-term arrangements between data holders and data recipients, for instance via a subscription model or the use of smart contracts, may reduce the costs in regular or repetitive transactions in a business relationship". In the meantime, some indicative timescales to govern commercial discussions would likely be helpful. Such timescales are commonplace in regulated sectors (e.g. provisioning timeframes for leased line circuits). These issues can still be controversial and are often raised in the context of dispute resolution proceedings.
Technical feasibility	A condition that typically limits the scope of a regulation on the basis that it is not provided by current technological capability (sometimes applied in electronic communications regulation, on topics such as access to calling line identification for emergency services).	The data sharing obligation in Article 5 is subject to a 'technical feasibility' condition. This is an area which is likely to create differences of opinion (also given the likely asymmetry of information between the data holder and the data recipient). Further guidance on how this consideration should be applied would likely be beneficial.
Economic viability	The extent to which the cost of meeting a request is proportionate given the high cost of doing so.	It is notable that Article 5 does not refer to the 'economic viability' of the data sharing. Concepts of 'technical feasibility' and 'economic viability' often go hand in hand, for example in telecoms regulation relevant to the provision of calling line identification for emergency calls. Economic viability also appears to be a relevant consideration in relation to data sharing. If a data holder could in theory update its systems to make the data available, albeit at a very significant cost, it begs the question of whether it would be economically viable, and therefore proportionate, to do this.
Trade secrets	Directive (EU) 2016/943 provides that the acquisition, use or disclosure of a trade secret shall be considered lawful notably where such acquisition, use or disclosure is required or allowed by Union or national law.	The Data Act is clear that trade secrets shall be preserved and shall only be disclosed provided that the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality. This was a particularly contentious point in the negotiation of the Regulation.

Conclusion

Key questions and strategic implications for data holders

Key Questions	Strategic Implications
Who should be involved?	Data holders should identify and, if necessary, upskill employees responsible for developing the company's commercial and technical strategy in this area and for conducting negotiations with data recipients.
What data should be shared?	Data holders will need to establish methods for identifying what data they could potentially be required to share with other businesses. This data identification process should be repeatable, used to assess any new data items, and keep track of any complementary data regulations (e.g., GDPR).
Are any changes required to existing processes?	Data holders should review and where required update their processes to comply with these requirements. This includes ensuring a transparent approach, as well as developing the processes and timescales relevant to negotiations with data recipients (e.g. new pricing approval processes).
How will the data sharing practically take place?	Data holders will need to design and implement the technical basis on which data will be retrieved and shared. Such data is required to be shared in a secure and commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time.
How much will be charged for data sharing?	A key strategic implication for data holders will be determining how rates should be calculated consistent with the FRND obligation. Data holders should consider whether this is included as part of a pricing methodology and indicative ratecard that can be shared with data recipients.
What additional governance structures are required?	It will be important for data holders to develop and share adequate management information relevant to the data sharing framework. This includes ensuring governance relevant to pricing strategies and management of dispute resolution processes.



Conclusion

How to prepare for Data Act compliance

Preparing for the data act in 3 steps

1. **Establish the current state and readiness** of the business for the Data Act, for example by completing a **gap analysis** **[see accompanying box]** against the key Act requirements. This should include:
   - Stakeholder interviews and documentation review;
   - Gap analysis against a reputable framework that includes key changes; and
   - Collation of findings and recommendations.
2. **Define business ambitions and risk appetite** in line with existing risk management policies. Define these in collaboration with senior stakeholders in order to ensure program buy-in.
3. **Develop a plan to close gaps** to meet business ambitions, either by updating processes or accepting certain risks. Include steps for monitoring any updates relevant to the obligations.

Key elements to consider in carrying out a gap analysis:

1. Review **data collection** and **data use strategies** and processes against the new Data Act obligations.
2. Review **readiness for the data sharing obligations** set out in the Act.
3. Analyse the proposed Act against other UK and EU regulatory obligations.
4. Assess the **amount of change needed** for Data Act compliance.
5. **Monitor** for updates (e.g. Implementing Acts or Guidance) relevant to the obligations in the Data Act.

Key contacts

EMEA Centre for Regulatory Strategy

Suchitra Nair
Partner
snair@deloitte.co.uk

Robert MacDougall
Director
rmacdougall@deloitte.co.uk

Matteo Orta
Senior Consultant
morta@deloitte.co.uk

Key EU contacts

Germany

Ljuba Kerschhofer-Wallner
Partner
lkerschhoferwallner@deloitte.de

Philip Zimmer
Director
pzimmer@deloitte.de

Netherlands

Simone Pelkmans
Partner
spelkmans@deloitte.nl

Oskar Mulder
Manager
omulder@deloitte.nl

Belgium

Matthias Vierstraete
Director
mvierstraete@deloitte.be

Willem-Jan Cosemans
Director
wcosemans@deloitte.com

Key UK contacts

Economic Advisory

Neil Clements
Partner
nclements@deloitte.co.uk

Anais Bauduin
Assistant Director
abauduin@deloitte.co.uk

Cyber, Digital, Data

Isabel Fitzpatrick-Pirie
Director
ifitzpatrickpirie@deloitte.co.uk

Selina Baechli
Senior Consultant
sbaechli@deloitte.co.uk

Internet Regulation

Nick Seeber
Partner
nseeber@deloitte.co.uk

Laurie Gilchrist
Director
lgilchrist@deloitte.co.uk

Deloitte.