# Study on the impact of the Data Act proposal on European telecom operators

Commissioned by etno

LE Europe

plum

wiggin

October 2022

## About LE Europe

LE Europe is one of Europe's leading specialist economics and policy consultancies. We advise an international client base throughout Europe and beyond on economic and financial analysis, litigation support, policy development and evaluation, business strategy, and regulatory and competition policy.

Our consultants are highly-qualified economists who apply a wide range of analytical tools to tackle complex problems across the business and policy spheres. Our approach combines the use of economic theory and sophisticated quantitative methods, including the latest insights from behavioural economics, with practical know-how ranging from commonly used market research tools to advanced experimental methods at the frontier of applied social science.

We are committed to providing customer service to world-class standards and take pride in our clients' success. For more information, please visit www.le-europe.eu.

**Office:** 35 rue du Congrès, 1000 Bruxelles, Belgique.

w: le-europe.eu
t: +32 2 229 19 02
e: info@le-europe.eu
f: +32 2 227 27 80
: @le_europe

## Authors

**Moritz Godel** Divisional Director

**Sam Wood** (Plum Consulting), Principal

**Victoria Harris-Honrado** (Wiggin) Partner

**Gordon Moir** (Wiggin) Partner

**Clio von Petersdorff** Economic Consultant

**Pietro Guglielmi** Economic Analyst

# Executive Summary

Following the publication of the European Commission's Data Act proposals in February 2022, ETNO, the European Telecommunications Network Operators' Association, commissioned LE Europe, in partnership with Plum Consulting and Wiggin LLP, to produce a study on the impact of the Data Act proposal on European telecom operators.

The study investigated how the proposed new rules will affect the – existing and emergent – business models operated by ETNO members in the business-to-business (B2B), business-to-consumer (B2C) business-to-government (B2G) and cloud and edge computing markets. Evidence for the study was gathered through a survey and interviews with ETNO members. The research was carried out over the summer of 2022.

## B2C and B2B data sharing provisions

This study demonstrates the existence of many diverse business models based on the free flow of data between businesses at different points of the data value chain. This market is already generating substantial value and innovation for European business and consumers.

In the B2B and B2C space, the study identified four distinct business models that are characterised by the different roles of telecom operators in the provision of connected Internet of Things (IoT) devices and related services, including differences in control over the data generated in the process.

The complexity of the data value chain means that any assumptions regarding the potential data-enabled market power of data holders or the privileged access to data based on an organisation's position in the value chain need to be carefully assessed on a case-by-case basis.

**Recommendations**

- Any regulation of these nascent markets should proceed with **caution.**
- The Data Act should support the competitive market by ensuring **fair compensation** on commercial terms for any data sharing between firms wherever possible. Accordingly, the Data Act should clarify responsibilities of different parts of the value chain (especially in relation to resellers of IoT devices) and recognise the full extent of the costs and liabilities involved.
- Key concepts in the Data Act require clarification to ensure the Act is appropriately targeted. "IoT devices", "virtual assistants", "product", "service management layer", and "related services" need to be clarified and explicitly state **what products/services are included and excluded.**
- Data generated by the operation of an electronic communications service ("ECS data"), including traffic data, location data and communication. **ECS data should be explicitly excluded from the scope of the Data Act,** as the existing regulation of collection and use of this data (notably the ePrivacy Directive) put it in a distinct category and must therefore be clearly distinguished from device data that has been generated using an IoT product or product related service.
- The Data Act proposal should therefore be harmonised and **coordinated with the ePrivacy rules,** to ensure there is no legal conflict between the Data Act and sector-specific rules pertaining to communications data, where confidentiality of communications considerations apply.

- The **same level of protection** should be granted to "products" and "related services".

## B2G data sharing provisions

Data held by private sector organisations can play an important role in the fulfilment of important tasks for the benefit of the public.

However, the provisions in the Data Act that deal with B2G data sharing are overly broad and risk excessive demands for data sharing from public sector bodies.

**Recommendations:**

- The **definition of concepts such as "public emergency" and "exceptional need for data"** need to be clarified and circumscribed.
- **Access obligations,** as a measure of last resort, **should be limited** to clearly specified cases of truly exceptional nature (e.g., officially declared public emergencies) and include safeguards that any data provided cannot be used for purposes other than the one for which it is requested.
- The Data Act should recognise that adequate **compensation** (cost recovery at a minimum) is required to incentivise ongoing investment in data infrastructures.

## Data processing service switching obligations

The market for data processing services is diverse and includes many multi-party business models for which a simple division into powerful sellers and weak customers is inaccurate.

Regulation should be sensitive to the real technical constraints that complex, high volume data processing services operate under, including in relation to switching. Rigid rules that assume that one size fits all are unlikely to meet the Data Acts pro-competitive objectives.

**Recommendations**

- The Data Act should **clarify who is responsible for the switching process in multi-party business models** and ensure that resellers, who are simply reselling a cloud service offered by a third-party, have a legal claim vis-à-vis said third-party to ensure the effective implementation of switching requirements for their customers.
- The Act should be modified so that cloud service providers and their enterprise customers can **agree on a different notice and switching period,** in particular if this benefits the customer.

# Table of Contents

# Table of Contents

Page

# 1 Introduction

## 1.1 Rationale of the Data Act

The overarching objective of the Data Act is to ensure fairness in the digital environment, stimulate a competitive data market, open opportunities for data-driven innovation and make data more accessible for all by facilitating data sharing for IoT devices and IoT-related services[1]. According to the European Commission, 80% of industrial data produced by connected devices is currently collected and never used. This underutilisation of data at the EU level leads to negative externalities for consumer choice, innovation, and public service delivery. The Data Act is intended to address the legal, economic, and technical problems that underpin the underutilisation of data generated by connected devices by creating a more predictable legal framework for access to data. This is supposed to prevent contractual inequities, streamline access to commercially held data by public sector agencies, promote switching between different providers of data processing services, and establish a framework for efficient data interoperability.

According to the Impact Assessment Report that accompanies the proposal, the new rules are expected to increase EU-27 GDP by 1.98 percentage points by 2028 and increase government revenues by EUR 96.8 billion. In addition, the Data Act is expected to increase investment activities by EUR 30.4 billion between 2024 and 2028 and bring about 2.2 million new jobs.[2]

The specific objectives of the Data Act proposal are the following:

- Chapter II, articles 3, 4 and 5 include measures to enable consumers and companies using connected products and related services to **access** more easily the data they produce and facilitate the access to such data for commercial re-use and innovation between businesses – these measures would generate up to EUR 196.7 billion a year by 2028 and cost EUR 410 million in one-off costs and EUR 88 million in recurring costs[3].
- Chapter V (articles 14-22) sets out obligations for making commercially held data available to **public sector bodies and institutions** in cases of exceptional need including public emergencies (such as floods and wildfires) – this measure would reduce the administrative burden by up to EUR 155 million and invoke EUR 552.5 million in one-off and EUR 78.1 million in recurring costs[4].
- Chapter VI includes measures to **facilitate switching** between Data Processing Services. At present there are barriers to switching between cloud services in the EU and there is limited ability to combine data emanating from different sectors. The Data Act aims to make it easier to switch between cloud service providers (incl. edge cloud) at no extra cost, based on new contractual obligations for providers and a new standardisation framework for data and cloud interoperability. This is estimated to generate an additional EUR 7.1 billion a year, at a cost of EUR 1 million per new standard[5].

[1] European Commission (2022) Data Act: Commission proposes measures for a fair and innovative data economy. Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

[2] European Commission (2022) Commission Staff Working Document – Impact Assessment Report. Available at https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act

[3] Ibid.

[4] Ibid.

[5] Ibid.

- As **SMEs** have less negotiation power than market leaders in data-sharing agreements, the Data Act includes provisions to prevent abuse of contractual imbalances in data-sharing contracts. It also intends to shield SMEs from unfair contractual terms unilaterally imposed by parties with significantly stronger bargaining positions. This measure is estimated to boost SMEs' profits by around EUR 5.2 billion a year, and generate an additional EUR 7.4 billion a year, at a cost of EUR 69 million a year[6].

The proposal also includes safeguards against **unlawful transfers** of non-personal data in response to a data request from a non-EU/EEA authority. In the Commission's plans, businesses will have more data available and benefit from a competitive data market; aftermarkets providers will be in the position to provide more tailored services and compete with comparable services offered by manufacturers; users of connected products could benefit from the presence of alternative and cheaper repair and maintenance providers (or maintain and repair them themselves), which could extend the lifecycle of products and contribute to the Green Deal objectives.

## 1.2 How the Data Act fits into the overall EU data policy landscape

The Data Act is proposed as a complement to the two other major policies that aim to facilitate a European single market for data: the Data Governance Act and the Digital Markets Act. The Data Governance Act focuses on mechanisms for data sharing and creates the processes and structures to facilitate data sharing by companies, individuals, and the public sector. On the other hand, the Data Act regulates who can use the data generated by connected products and related services, and what the conditions are for such use. The Digital Markets Act (DMA) deals with fair competition between gatekeepers and other market players, and with portability obligations for cloud service providers. However, the DMA's portability provisions are limited to end users and cannot be invoked by business users. Moreover, the Commission believes that further regulation is needed due to vendor lock-in issues that reach further than gatekeepers. The Data Act, therefore, includes a framework of minimum conditions to enable switching which would apply horizontally across the market and preserve the asymmetric approach of the DMA versus gatekeepers.

Under Article 20 of the GDPR, the right to receive personal data held by a controller and transfer it to another one is limited to personal data processed on certain legal bases and where technically feasible, and portability between cloud providers is largely out of scope. The Data Act will enhance the right to data portability for connected products so that consumers can access and transfer any data generated by the product and services they use, both personal and non-personal, permanently and in real-time.

Another important relationship is with the Free Flow of Non-Personal Data Regulation (FFoD) which ensures that non-personal data can be stored, processed, and transferred anywhere in the EU. The FFoD also deals with the issue of 'vendor lock-in' at the level of providers of data processing services, using a self-regulatory approach under which providers abide by a code of conduct to facilitate transferring data to an alternative cloud service. The Data Act introduces a regulatory approach to facilitate the exercise of this switching in practice.

The Data Act does not have specific overlaps with the Digital Services Act (DSA), but they both share the objective of rebalancing the digital economy towards smaller economic agents and of empowering the users of digital services. One of the major goals of the Data Act is to make sure that

[6] European Commission (2022) Commission Staff Working Document – Impact Assessment Report. Available at https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act

the biggest online service providers ('gatekeepers'), which are the target of the DMA and the DSA, are not the main beneficiaries of the new rights on data access and portability.

Finally, the Data Act revisits certain parts of the Database Directive, which was conceived in 1996 to protect investments in the structured presentation of data. Under the Data Act, the Database Directive cannot be the legal basis to prevent data generated by a connected product or related service from being accessed.

## 1.3 Who will be affected by the Data Act

According to the European Commission, the following are the stakeholders that will be affected by the Data Act:

- **Original equipment manufacturers (OEMs)** of devices able to collect or generate data and communicate it. According to the Commission, around 300,000 EU companies fall in this category: Medium and large OEMs will face costs related to compliance, legal advice, and adaptation of their products' design; they may also lose their advantage in aftermarkets. Medium and large companies could also face compliance costs related to increased data requests from governments, but these may be offset through consistency of the requests and reduced duplication. The proposal specifies that smartphones, tablets, and webcams are excluded from the scope along with other devices that require human input to produce various forms of content.
- **Companies and consumers using such devices** would benefit from the presence of more providers of repair and maintenance services, which might prevent them from having to buy new products. All consumers would be able to get access to all data generated by their connected products and could choose what to do with it, while currently this right is limited to personal data processed based on consent or contract.
- Around 716,000 **third-party businesses** could reuse data generated by connected products, and are expected, through interoperability measures, to save 30% of data-processing costs and avoid the loss of 40% of valuable data sharing.
- It would be easier for **public sector agencies and institutions** to obtain data held by private providers when they are needed for situations of exceptional need including in public emergencies.
- **Businesses that use cloud services** will face lower prices because of the data interoperability requirements, with benefits estimated to reach EUR 7.1 billion per year.
- Most aftermarket service providers are **SMEs**, who are likely to be more reliant on third-party data than large companies. Through the Data Act, they would be shielded from unbalanced contract terms. SMEs would generally be exempt from data-sharing obligations in the context of data generated by machines and the use of products, and from B2G obligations.
- **Standardisation bodies** tasked with developing interoperability standards are estimated to incur approximately EUR 1 million per standard.

# 2 B2C and B2B data sharing provisions

This section describes ETNO members' business models that are likely to be most heavily impacted by chapters II, III and IV of the Data Act. It is informed by interviews with ETNO members, desk research and analysis of the draft Data Act.

Chapter II of the Data Act sets out obligations for making available data generated using *products*, *related services,* or *virtual assistants*. These are defined in the Data Act as follows:

- 'data' means "*any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording*";
- the 'data holder' is "*a legal or natural person who has the right or obligation, in accordance with [the Data Act and applicable 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*";
- a 'product' means a "*tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data*";
- a 'related service' means "*a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions*"; and
- 'virtual assistants' means "*software that can process demands, tasks or questions including based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access to their own and third party services or control of their own and third party devices*".

The obligations in respect of these include:

- the obligation to design and manufacture products and related services in such a manner that data generated by their use are directly accessible to the user (Article 3);
- the obligation for the data holder to make available to the user data generated by their use of a product or related service (Article 4); and
- the obligation to, upon request by a user or by a party acting on behalf of a user, make the data generated by the use of a product available to a third party (Article 5).

Chapters III and IV further clarify the scope of these obligations as well as related technical protections and dispute resolution provisions.

### Box 1 Recommendations regarding the B2B and B2C data sharing provisions

The market for connected devices, related services and the data they generate is still in an early stage of development. Any **regulation of these nascent markets should proceed with caution**.

The Data Act should recognise that **the market for data sharing, though in very early stages of development, exists and is already generating value added and innovation based on shared data.** There are many diverse business models based on the free flow of data between businesses at different points of the data value chain. The Data Act should support the competitive market by

**ensuring fair compensation on commercial terms for any data sharing between firms** wherever possible. This means the Data Act should:

- Clarify who will bear the legal costs (data will have to be checked and verified, possibly requiring input from a legal professional) the data provider will incur, e.g. to ensure that data is non-personal or doesn't infringe an intellectual property rights before sharing them with other businesses or consumers;
- Clarify the responsibilities of resellers of IoT devices, for example, a situation where a firm (such as a telecom operator) is selling an IoT device that is manufactured by another party, and this OEM controls the technical specification of the device (but hasn't got access to the data);
- Clarify who is liable if data is misinterpreted, lost, or used by data recipients for nefarious purposes;
- Take into account the costs associated with extracting data from devices on demand, including the costs associated with building and maintaining Application Programming Interfaces (APIs) to allow third parties access to data collected from IoT devices and the opportunity costs for the time and resources spent by data holders on fulfilling the obligations set out in the Data Act.

Key concepts in the Data Act require clarification to ensure the Act is appropriately targeted. "IoT devices", "virtual assistants", "product", "service management layer", and "related services" need to be clarified and explicitly **state what products/services are included and excluded.**

Data generated by the operation of an electronic communications service ("ECS data"), including traffic data, location data and communication. **ECS data should be explicitly excluded from the scope of the Data Act,** as the existing regulation of collection and use of this data (notably the ePrivacy Directive) put it in a distinct category and must therefore be clearly distinguished from device data that has been generated by the use of an IoT product or product related service.

The Data Act proposal should be harmonised and coordinated with the ePrivacy rules, to ensure there is no legal conflict between the Data Act and sector-specific rules pertaining to communications data, where confidentiality of communications considerations apply.

There is no rationale for different levels of protection for 'products' (Art, 4(4)) and "related services". Granting **the same level of protection for manufacturers and service providers** would support the objective of the Data Act to facilitate after-market competition, by enabling data access for the development of new and innovative products and services, while protecting data holders from unfair competition.

## 2.1 Affected business models

The Data Act provisions affect those business models which offer connected Internet of Things (IoT) devices and related services. These business models cover a wide range of consumer and industrial applications. In many cases, a device itself will not allow direct access to any data it generates. This may be the case, for instance, in devices with a small form factor, limited computing power and/or lack of a user interface (for example, a connected sensor).

The Data Act also affects business models offering 'virtual assistants', defined in the Act as "*software that can process demands, tasks or questions including based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access to their own and third party services or controls their own and third party devices*." (Art 2(4)). This is a broad definition which could potentially include a wide variety of different software platforms and even applications for controlling connected devices.

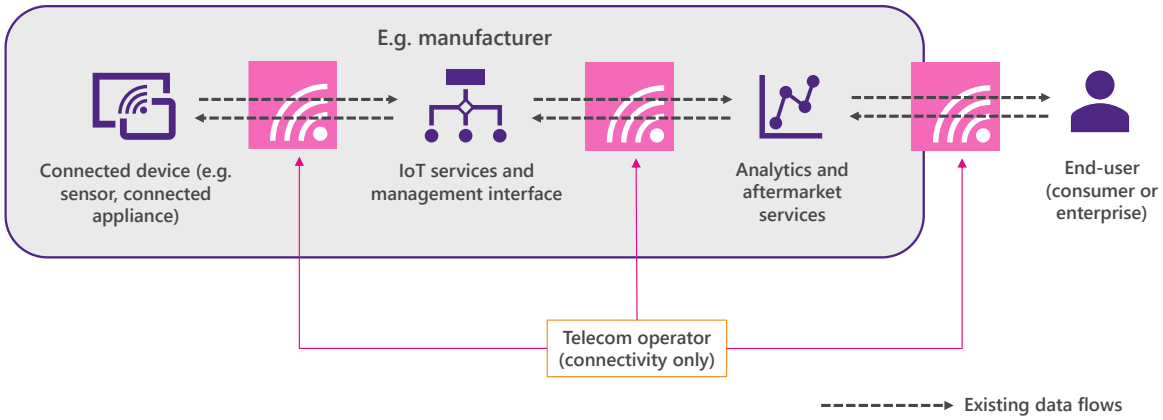
Rather than provide an exhaustive breakdown of all the possible applications of IoT services, we have instead focused on the mechanisms in which these products and services are delivered, which may impact members' exposure to the relevant provisions of the Data Act. We illustrate how each mechanism functions in practice by way of examples.

### 2.1.1 Connectivity (only) supplied by telecom operators

A common type of business model is one where only connectivity is supplied by the telecom operator, with connected hardware and related services provided by another entity. These IoT connectivity services are an important part of many operators' business offerings, used in a wide range of civil and enterprise contexts.

One example of this type of model is in the automotive sector: the auto manufacturer will often build in connected sensors and embedded SIMs[7], manage the collection of data, and supply related services (e.g., aftermarket maintenance).[8] To enable the necessary data flows, the auto manufacturer will use global connectivity services provided by a telecom operator.

**Figure 1 Business Model 1A – connectivity (only) is supplied by telecom operators**




In such cases, the operator will only hold data pertaining to the use of its network, rather than data generated by the device itself. Moreover, network data is not equivalent to data generated by connected devices and may represent only a partial picture (e.g., if a connected car changes network in transit).

The telecoms operator involved in this business model only has access to Electronic Communication Service (ECS) data and the role of ECS connectivity services is simply to enable many smart devices to communicate with other devices and services (as a medium for transmitting data). In other words, ECS are not "related to" a specific functionality or product. It is important to distinguish between data generated by a connected device and data generated from a device's use of a communications network - the Data Act is ambiguous on whether the latter data are in scope.

[7] Embedded Subscriber Identity Module (eSIM) technology (also known as eUICC) can be built in during the manufacturing process and configured remotely to provide connectivity across multiple mobile network operators. Refer to: https://www.ericsson.com/en/blog/2020/9/esim-driving-global-connectivity-in-the-automotive-industry

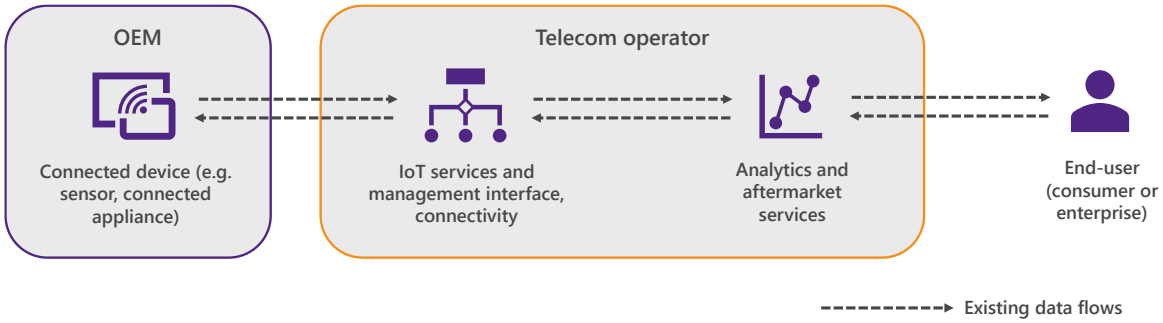
[8] Note, however, that in this example there is a lack of clarity in the Data Act about the nature of the 'product': whether it is the car itself, the eSIM or the sub-components (e.g. sensors) which gather data.

If these data on network use are not in the scope of the regulation, then neither are such business models. However, if these data are included in the scope, then the impact of the Data Act in this scenario would be to risk creating disproportionate regulatory obligations for telecommunications service providers, in light of the intended purpose of the Act (to open access to device data which was previously exclusively held by manufacturers of connected devices). It also raises the prospect of a conflict between the Data Act and the ePrivacy Directive, which governs ECS data.

### 2.1.2 Only related services are supplied by the telecom operator

A different scenario can arise when the connected hardware is provided by a third party, while the telecom operator supplies related services (such as a management platform or data analytics services) and/or connectivity. This is illustrated in Figure 2.

**Figure 2 Business model 1B– related services provided by telecom operator; hardware supplied by 3rd party**




In this scenario, data generated by the connected device are collected by an IoT management platform, from which they can be accessed by the end-user. These data may be stored on behalf of the end-user or stored on the end-user's own infrastructure. The management platform may also be used to monitor the connected devices and to issue actions.

This model can apply to both the consumer and enterprise space:

- In the **consumer space**, related services include Smart Home applications that allow consumers to manage and control their connected devices (including devices supplied by third parties). Examples here include Telia's Smart Family app[9] and Orange Belgium's Smart Home app.[10] or Deutsche Telekom's MagentaZuhause smart home app.[11] In some instances, such applications also include voice control which means that they might fall under both the 'related services' and 'virtual assistants' categories in the Data Act respectively.
- In the **enterprise space**, examples include Deutsche Telekom's 'Cloud of Things' IoT management platform[12] or Orange's 'Live Objects' platform.[13] Such platforms can be used to support a wide range of enterprise verticals, including manufacturing applications, smart logistics, smart agriculture, and smart cities

[9] https://play.google.com/store/apps/details?id=com.teliacompany.zone&hl=en_GB&gl=US

[10] https://play.google.com/store/apps/details?id=com.orange.be.smarthome&hl=en_GB&gl=US

[11] Refer to: https://www.smarthome.de/

[12] https://iot.telekom.com/en/solutions/platform

[13] https://www.orangefab.ro/en/news/innovation/orange-launches-live-objects-iot-device-management-platform/

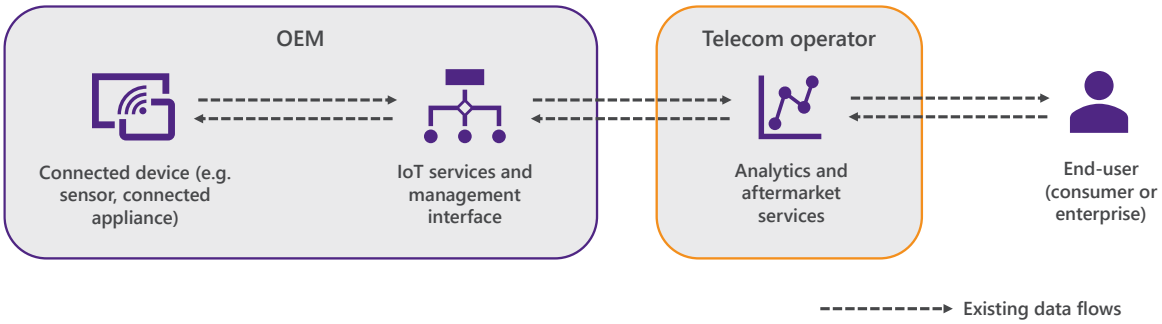
We understand that among ETNO members, enterprise applications are the more common.

### Box 2 Case study: Urban Genius by TIM[14]

TIM's Urban Genius is a platform for managing Smart City systems, and for optimising and generating insights from those systems. Urban Genius can work with pre-existing smart city systems – for example 'smart parking'. The platform can integrate data streams from these systems, which can then be analysed with AI-powered tools supplied by the operator.

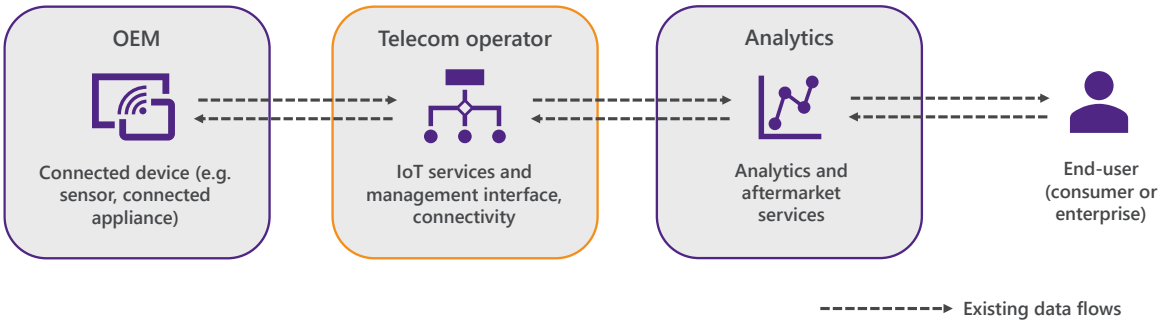
A variant of this model is when the device manufacturer also provides its own proprietary management interface for controlling and collecting data from the connected devices it supplies (Figure 3). Data may then be forwarded to the telecom operator for data analytics.

**Figure 3 Business Model 1B (II) – hardware and management platform supplied by device manufacturer; analytics supplied by telecom operator**




Another variant of the model is one in which the telecom operator supplies the management platform for controlling connected hardware, with data analytics and related aftermarket services provided by a third party (Figure 4). This type of model may also potentially include software applications used to control connected devices if they are deemed as 'virtual assistants', though this is ambiguous in the Data Act.

**Figure 4 Business Model 1B (III) - hardware supplied by device manufacturer, management interface supplied by telecom operator, analytics and aftermarket services supplied by 3rd party**




The key commonality across these models is that the telecom operator is not the supplier of the connected hardware but is supplying a related service.

[14] Refer to: https://www.olivetti.com/it/iot-big-data/soluzioni-iot/tim-urban-genius

There is a degree of ambiguity in the Data Act over which actor would be deemed a *data holder* in these situations. In particular, the definition of 'related' services is at present relatively ambiguous and not restricted to services that are directly related to the product offering, e.g., as part of the sales, rent or lease agreement. While Recital 16 notes that "related services" can capture services that are "normally provided for products of the same type and the user could reasonably expect them to be provided" – this wording is vague and would risk including services that are provided by third parties which are entirely independent from the original product.

It is possible that telecom operators would be considered *data holders* in some situations, depending on the context and nature of the services supplied. However, if some data requests are directed at other actors (i.e., device manufacturers or third-party analytics services) the impact on telecom operators should be reduced relative to models where the operator supplies both hardware and related services.

### Box 3 Business model 1B: Case study

**Orange** provides the French utility company Veolia with an IoT service to collect data from Veolia intelligent water meters through Orange's LoRa network and manage the data collected through Live Objects (Orange's data management platform). Orange's LoRa network covers over 30,000 municipalities and 95% of the population of Metropolitan France and is effective in the case of intelligent meters, which are often located in hard-to-access environments, such as building basements or within meter access hatches.

**Deutsche Telekom** worked with the German independent auto parts wholesaler Select AG to create a solution to compete with automakers in the market for maintenance and repair. Since 2018 German cars must have a sim installed that can send an emergency signal in the case of an accident. This has allowed auto manufacturers and their authorised workshops to receive all vehicle condition data automatically, which enables them to contact their customers directly and inform them about upcoming repairs. This gives them a competitive advantage over independent garages. DT has provided Select AG with an IoT platform that allows them to offer independent garages the possibility to allow their customers to connect their cars to the independent garage's platform (rather than the automaker authorised workshops') which enables them to analyse vehicle data and approach customers about preventive maintenance in a more targeted way.

#### DT's Cloud of Things

The Cloud of Things[15] is DT's cloud based IoT application platform for the Internet of Things. It is a solution to connect devices and machines while monitoring and controlling them remotely. The Cloud of Things collects the sensor data of connected machines in real-time, analyses it, and provides an overview of several parameters, such as pressure, temperature, or position. It also allows for remote maintenance, setting of rules & alarms, and data analytics.

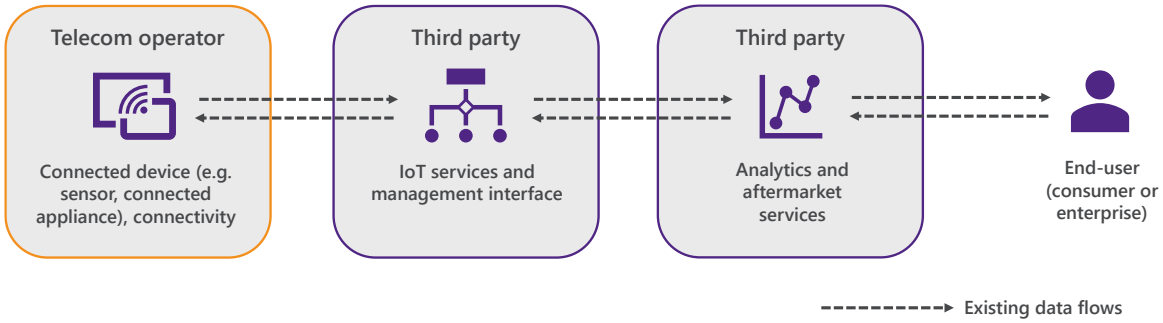

**TIM** provides the same services outlined in section Box 5 also independently from the hardware - customers sometimes select hardware providers autonomously and require system integration to allow interoperability between hardware and platform, as in the case of connected cars.

[15] DT - Deutsche Telekom, https://iot.telekom.com/en/solutions/platform

### 2.1.3 Only hardware is supplied by the telecom operator

This model represents the inverse situation to the previous one: the telecom operator supplies a connected device, which the end-user controls using a management platform from a third party (such as a tech firm).

**Figure 5 Business Model 1C – hardware supplied by the telecom operator; related services (except connectivity) supplied by 3rd parties**




This scenario has several variants:

1) Some operators offer connectivity and connected hardware as part of a service bundle, for example, a connected tracker for the consumer market. For the enterprise market some operators provide both M2M connectivity and an IoT gateway. We understand, however, that it is more common for operators to supply hardware in conjunction with an IoT management platform (i.e., Model 1D, see below).
2) Some operators offer connected devices as standalone products, which are often interoperable with numerous management platforms.[16] However, in this situation, the operator is typically the vendor, rather than the manufacturer of the device, and will neither hold the data generated by the device nor be in control of the technical design.
3) The end-user may have purchased a service package including both connected devices and management software from an operator, but subsequently opted to use a different management platform to control the connected devices.

The Data Act is ambiguous about which devices would fall under the scope of a 'product' in Article 2 (2) and how they are to be distinguished from the list of IT devices that are not covered by the Regulation according to Recital 15 or from other devices that facilitate connectivity (such as IoT gateways).

Additionally, it is not clear what constitutes a 'manufacturer' of a product as per Article 3 (1). It is unclear whether a telecom operator that is simply reselling a product and is not involved in the design or manufacturer of the product concerned, is within scope of the Data Act.

It is therefore possible that the telecom operator could be considered a *data holder* in this scenario. However, it is likely that in many cases, the telecom operator will neither hold data generated by the device nor be in control of the technical design of products it sells. In such cases the customer will have control of any data generated by their device.

[16] For example, Vodafone Ireland. Refer to: https://vodafonefaf.ie/collections/connected-home

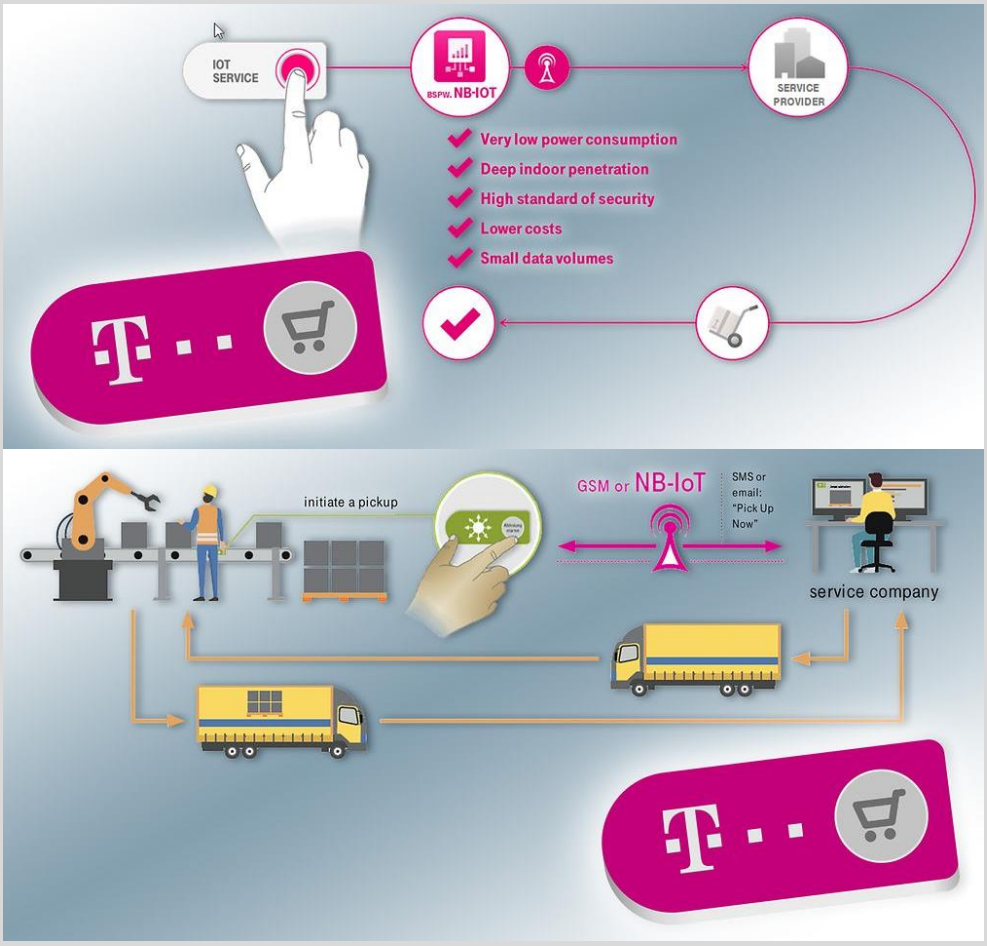
### Box 4 Business model 1C: Case study

**TIM** provides IoT gateways and Machine-to-Machine (M2M) connectivity for several IoT verticals, including gas and water metering, insurance telematics, connected cars, exposing collected data through Application Programming Interfaces (APIs), or sending data into 3rd party platforms.

**Telefónica** sells solutions that include a device plus connectivity or a Printed Circuit Board (PCB) plus connectivity. The customer accesses the device to get operational data (configuration) and business data (sensors). The network transports data from and to the device.

**Deutsche Telekom** offers global network connectivity across 188 destinations, potentially in combination with smaller tracker solutions (e.g., service buttons).

#### DT's Service Button

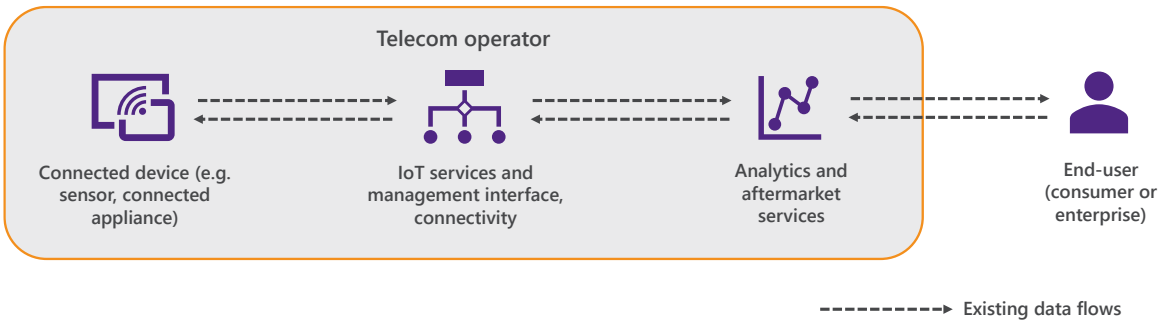



*Source: Deutsche Telekom, https://www.telekom.com/en/company/details/services-at-the-push-of-a-button-592224*

### 2.1.4 Both connected hardware and related services supplied by a telecom operator

Perhaps the most straightforward business model is one in which both the connected device and the related service are supplied by the telecom operator. This is illustrated in Figure 6.

**Figure 6 Business model 1D - Both connected hardware and related services supplied by a telecom operator**




In this model, the operator supplies the connected hardware and related services for managing the hardware (e.g., a management platform). The operator may also supply other related services such as data analytics and insights.

Both hardware and related services may be supplied as part of a service package to the end-user, which also includes connectivity. This business model is employed in a wide variety of contexts. Consumer applications include connected cameras, thermostats and plug adaptors. Enterprise applications include smart logistics, fleet management, smart agriculture solutions, and remote monitoring of distributed assets. We understand that, for ETNO members, enterprise applications are the more significant.

In many cases, the data generated by the device will already be available to the end-user via the related service or management platform (indeed, this is often a key motivation for the adoption of IoT technologies in the first place).

As the operator controls the technical design of the product and related services it would be considered the *data holder* under the Data Act and therefore could be subject to new data access requests under the Act.

### Box 5 Business model 1D: Case study

**Orange** provide IoT connectivity and devices for B2B markets through their subsidiary Orange Business Services' platform Live Objects[17] which allows industries to manage their connected objects, communicate with them, and process and analyse the collected data[18]. An example of the implementation of Live Object is its application together with the LTE-M (Long Term Evolution for Machines) network and a BOX2M[19] power management infrastructure to cover the energy dispatch requirements of a public authority in Romania. The installed infrastructure allowed rapid identification of phenomena such as the imbalance between the power phases of the public lighting system caused by an unequal load in the various stages of the system or exceeding the standard power quality parameters at certain time intervals, which could directly affect the operating time of

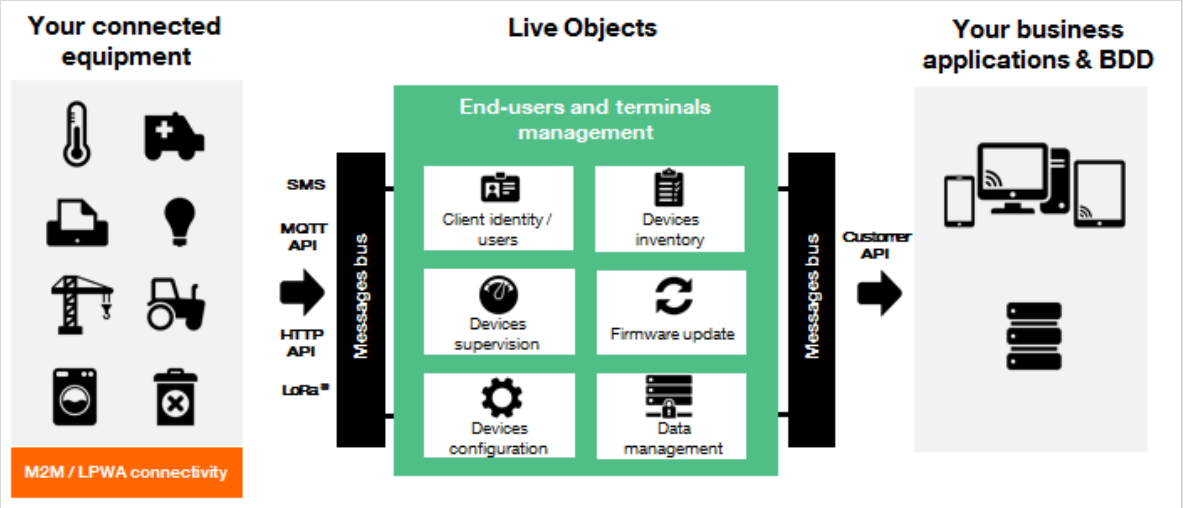
[17] https://www.orange-business.com/en/products/live-objects

[18] Live Objects could fall both under business models 1A and 1B, given that in some cases it is provided independently from the hardware (while sometimes Orange only acts as the reseller of hardware produced by other suppliers)

[19] https://www.box2m.com/

the connected equipment. Live Objects allowed to visualise and administer energy management reports, high-precision estimation of consumption, and all data generated by the system.

**Orange's Live Objects**




*Source: Orange, https://www.orange-business.com/en/products/live-objects*

**Orange** also supplied Safran Aircraft Engines with a smart tracking, IoT solution that included 15,000 trackers and 250 antennas to locate and manage all tools and equipment remotely and in real-time in two large industrial sites. Orange acted both as an operator and as an integrator and provided a solution to optimise the management and preventive maintenance of Safran's tooling fleet. The hardware was provided through suppliers of geolocation technologies in an industrial environment.

Another example from **Orange** is their vehicle fleets management service Ocean[20], which is a solution to optimise driver management, manage vehicle maintenance and geolocate equipment. Through the installation of a small tool in each vehicle, Ocean can be used e.g., for GPS tracking of construction machinery, to optimise the geographical coverage of sales forces, and by local authorities to monitor the response times, location of staff, and time spent in each location.

**A1 - Telekom Austria** provided Rail Cargo Austria with an end-to-end IoT solution to collect information about the position and movement of its wagons throughout Europe through tracking and tracing. Wagons have been equipped with SmartCargo devices, which have motion sensors for positioning and a 3D acceleration sensor for shock detection. The devices provide the GPS coordinates of the freight wagons at predefined intervals during the transport of goods. A definable geofencing can be used to monitor when a wagon crosses national borders or leaves a station, for example. At regular intervals, A1 Digital's M2M SIM cards installed in the devices transmit all information over the mobile network to an IoT platform. The SIM cards are managed through the SIM management platform provided by A1 Digital. In the absence of network coverage, the data transfer hardware also has an SMS fall-back. The incoming data is processed and visualised on the IoT platform.

[20] https://ocean.orange-business.com/ocean-society

**A1's SmartCargo**


***Source: A1 - Telekom Austria, https://www.a1stories.com/blog/the-train-is-on-the-move/***

**Deutsche Telekom** offers the Magenta Zuhause smart home app, an application/platform that can connect with and integrate the ecosystems of different device manufacturers and thus is not limited to DT-branded devices[21]. However, DT is also selling (and bringing to market) some devices (e.g. contact sensors, routers, adapters).

**TIM** developed IoT Smart Farm in collaboration with Olivetti, which is a cloud solution that offers companies a complete system of tools and information for precise monitoring of the physiological state of crops, irrigation needs, and crop yields. The data is collected by a network of sensors in the field and then sent to a platform that controls all the relevant parameters and intervenes when needed.

TIM provides other IoT solutions including remote monitoring of distributed assets (towers, sites, cabinets), industrial IoT applications, and smart city applications.

## 2.2 Impact of B2C and B2B data sharing provisions - European Commission proposal

Several parts of the Data Act are open to multiple interpretations. These ambiguities concern the type of data that is in scope, how the Data Act will interact with other legislation such as privacy legislation, and the definitions and scope of "related services", "products" and "virtual assistants". These factors will greatly affect how the B2B, and B2C data sharing requirements will impact the different business models outlined above.

[21] DT also provides the application independently from the hardware, which means that Magenta Smart Home can also fall under business model 1B

### 2.2.1 Business models where connectivity is supplied by telecom operators

In all the business models described above, telecom operators supply connectivity. The role of connectivity is to enable smart devices to be connected and communicate with other devices and services. ECS are not "related to" a *specific functionality* or product and should, together with connectivity data (e.g., mobile caller location information), be clearly distinguished from the "product" and "related services" definitions within the scope of the IoT data sharing obligations in the Act. Without such a clarification**, the impact of the Data Act would be to risk creating onerous and disproportionate regulatory obligations for telecommunications service providers**, contrary to the intended purpose of the Act.

The Data Act proposal should also be harmonised and coordinated with the ePrivacy rules, to ensure the position is clear for communications data, where confidentiality of communications considerations apply. We note this is the intention of the EU Data Act, as Recital 7 mentions.[22]

On ePrivacy rules, to date, Directive 2002/58/EC (as amended) on the processing of personal data and protection of privacy in the electronic communications sector (the "ePrivacy Directive") ensures the confidentiality of communications and related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. Strict rules apply to prohibit the storage of communications and related traffic data without user consent, unless a lawful exception applies – e.g., public safety, to safeguard national security. Specific provisions also apply such that traffic data relating to subscribers and users processed and stored by public electronic communications networks or service providers must be erased or made anonymous when no longer needed for the transmission of a communication, subject to limited exceptions – such as processing for subscriber billing and interconnect payments. Rules on location data other than traffic data also apply, meaning, for example, that such data may only be processed when made anonymous, or with the consent of users or subscribers to the extent and for the duration necessary for the provision of a value-added service. It should be noted that a new "ePrivacy Directive" currently being negotiated looks to continue the same approach to ensure confidentiality of communications for both natural and legal persons. In the version of the proposed regulation accepted by the Council of the EU in Feb 2021, the new rules seek to apply to certain "Internet of Things services" scenarios as noted in Recital 12.[23]

There is a need for greater clarity in the EU Data Act on how ePrivacy rules apply to public electronic communications services (to ensure throughout the text the providers are clear on the need to

[22] Recital 7: *"(7) The fundamental right to the protection of personal data is safeguarded in particular under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725. Directive 2002/58/EC additionally protects private life and the confidentiality of communications, including providing conditions to any personal and non-personal data storing in and access from terminal equipment. These instruments provide the basis for sustainable and responsible data processing, including where datasets include a mix of personal and non-personal data. This Regulation complements and is without prejudice to Union law on data protection and privacy, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC. No provision of this Regulation should be applied or interpreted in such a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communications."*

[23] Recital 12: *"(12) The use of machine-to-machine and Internet of Things services, that is to say services involving an automated transfer of data and information between devices or software-based applications with limited or no human interaction, is emerging. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, this Regulation, in particular the requirements relating to the confidentiality of communications, should apply to the transmission of such services. The transmission of machine-to-machine or Internet of Things services regularly involves the conveyance of signals via an electronic communications network and, hence, constitutes an electronic communications service. This Regulation should apply to the provider of the transmission service if that transmission is carried out via a publicly available electronic communications service or network. Conversely, where the transmission of machine-to-machine or Internet of Things services is carried out via a private or closed network such as a closed factory network, this Regulation should not apply. Typically, providers of machine-to-machine or Internet of Things services operate at the application layer (on top of electronic communications services). These service providers and their customers who use IoT services are in this respect end-users, and not providers of the electronic communication service and therefore benefit from the protection of confidentiality of their electronic communications data. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU"*

protect the privacy of communications data, where required under ePrivacy rules). Specific confidentiality of communications requirements needs to be applied to the transmission of internet of things services via a publicly available electronic communications service or network, to ensure compliance with ePrivacy rules. IoT service providers (who operate at the application layer), and electronic communications service providers will need to consider rules applying to the protection of confidentiality of their electronic communications data when considering any Data Act request.

### 2.2.2 Business models where a related service is provided by telecom operators

Telecom operators provide related services, such as aftermarket services and/or analytics, in addition to connectivity in business models 1B and 1D. The size of the impact on these business models will be affected by the interpretation of "related services", when the regulation should apply, and what types of datasets are in scope.

Article 3 (1) requires that "*Products […], **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."* The purpose of the Act is to capture specific "related services" to a defined "product" scope – namely "a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions." Some services such as companion apps (e.g., a fitness tracker that comes with a dedicated app) can form an integral part of the product experience and functionality of an IoT device and fall within the scope of the 'related services' definition. However, what is less clear is what is meant in practice by a service being "incorporate[d] in" or "interconnected" in such a way that its "absence" would mean the product could not perform one of its functions. This definition is potentially very broad in scope.

**The definition of related services should be more clearly addressed to services that are directly related to the product offering**, for example as part of the sales, rent or lease agreement. Different business models and contexts could apply given emerging digital markets and technology, so more legal certainty is required on what is potentially in and out of the scope of data sharing obligations. While Recital 16 notes that "*related services"* can capture services that are "*normally provided for products of the same type and the user could reasonably expect them to be provided*"– this does not go far enough. This wording is too vague and would risk including services that are provided by third parties which are entirely independent of the original product.

The definition of virtual assistants in Article 2(4) and Article 7(2) is also ambiguous as to how the scope of the Act is delineated. This definition should be modified to clarify how a virtual assistant is defined, for example by specifying the modes of interaction which sets virtual assistants apart from a typical software application. This would provide more certainty to operators and help to clarify the scope of the Act.

In addition, the text at the end of Recital 16 is not appropriate where it mentions that "*This Regulation should also apply to a related service that is not supplied by the seller, renter, or lessor itself, but is supplied, under the sales, rental, or lease contract, by a third party. In the event of doubt as to whether the supply of service forms part of the sale, rent or lease contract, this Regulation should apply*." [emphasis added]. **Providers need legal certainty on the scope of the Data Act** and cannot be expected to simply assume that a scenario is covered – particularly given the fact that several very specific fact bases could apply, and the market and the data generated are in their infancy.

In our view, the Act should also be **clearer on the exact datasets that could be caught by a "service/management layer"** to help clarify this for telecom operators. Recital 14 of the Data Act

draws an important distinction on this point – noting "*Physical products that obtain, generate, or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation… Such products may include vehicles, home equipment and consumer goods, medical and health devices, or agricultural and industrial machinery."* While accepting that *"The data represent the digitalisation of user actions and events and should accordingly be accessible to the user"* Recital 14 goes on to note *"while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation. Such data are potentially valuable to the user and support innovation and the development of digital and other services protecting the environment, health, and the circular economy, in particular through facilitating the maintenance and repair of the products in question*." As telecoms operators could potentially be involved with platforms which "derive or infer" information from data, greater legal certainty is required on what this means in practice.

### 2.2.3 Business models where hardware is provided by telecom operators

In business model 1C and 1D telecom operators provide hardware in addition to connectivity. The impact on these business models will depend on the interpretation of a "product". Furthermore, not all hardware will have the technical features required to facilitate data sharing.

Article 3 of the Act contains an obligation "to make data generated by the use of products accessible." Article 3(1) requires that "**products** shall be designed and manufactured […] 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." As noted above, it would be helpful to have greater clarity in the Act on which devices would fall under the scope of a 'product' in Article 2 (2) and how they are to be distinguished from the list of IT devices that are not covered by the Regulation according to recital 15.

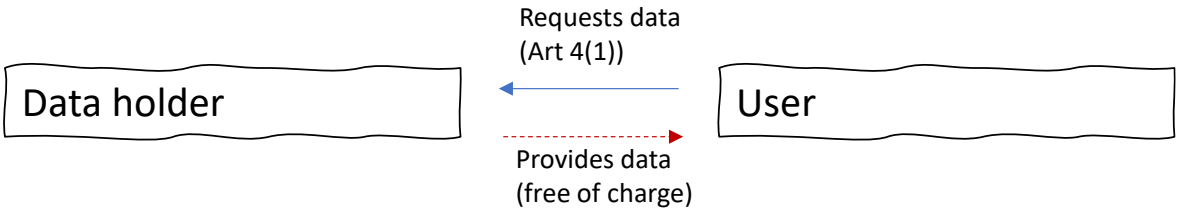
Article 3(1) is directed at the manufacturer of the product (given the reference to "design and manufacturer). In this scenario, if a telecom operator is not involved in the design or manufacture of the product concerned (and instead simply supplying the connected device (e.g., sensor, connected appliance) concerned), we believe they should be excluded from the data sharing obligation and would ask that this be clarified in the legislation.

One other key consideration on hardware is whether it is technically (and economically) feasible for a connected device to enable data sharing. Certain smaller devices do not have a user interface – so this should be allowed for under the data sharing rules.

### 2.2.4 Compensation mechanisms for data holders

The EC's impact assessment stresses that "*it is [also] important that entities that have invested in data generation continue to be fairly rewarded for these investments and are shielded against an increased risk of unlawful access to data*".[24]

[24] Commission Staff Working Document – Impact Assessment Report, SWD (2022) 34 final, available at https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act .



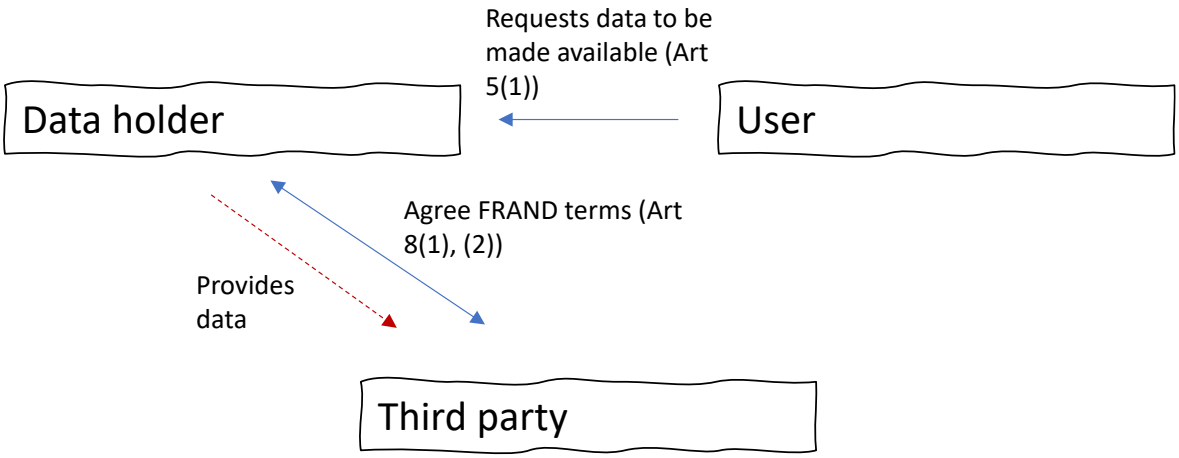

However, the stipulation in Art 4(1) that the data holder must make data available to the user free of charge is not incentive compatible and discourages investment in data infrastructure that provides value to users. At the same time, users are likely to end up indirectly bearing at least some of the cost of data provision.

Since the proposals don't restrict the ability of data holders to spread the (fixed) cost of data sharing across their user base, they encourage a suboptimal pricing structure, combining underinvestment in sharing infrastructure (which harms users with large and complex needs, since they can't be priced on a case-by-case basis), and unnecessarily high prices for users that do not request data via Art 4(1).

At the same time, a third-party recipient of user data from a data holder can pass on the cost of data access (the compensation agreed with the data holder) to the user, resulting in a situation where some users incur different costs for the same service depending simply on whether the service is provided in-house (where Art 4(1) specifies the relevant data is provided free of charge) of outsourced to a third party (where the user can be charged by the third party service provider who received the data under Art 5(1). As observed by the Max Planck Institute (2022, para (72)), this is likely to disadvantage mainly smaller firms, who are less likely to have the capabilities to provide the data-enabled value-added service in-house.[25]

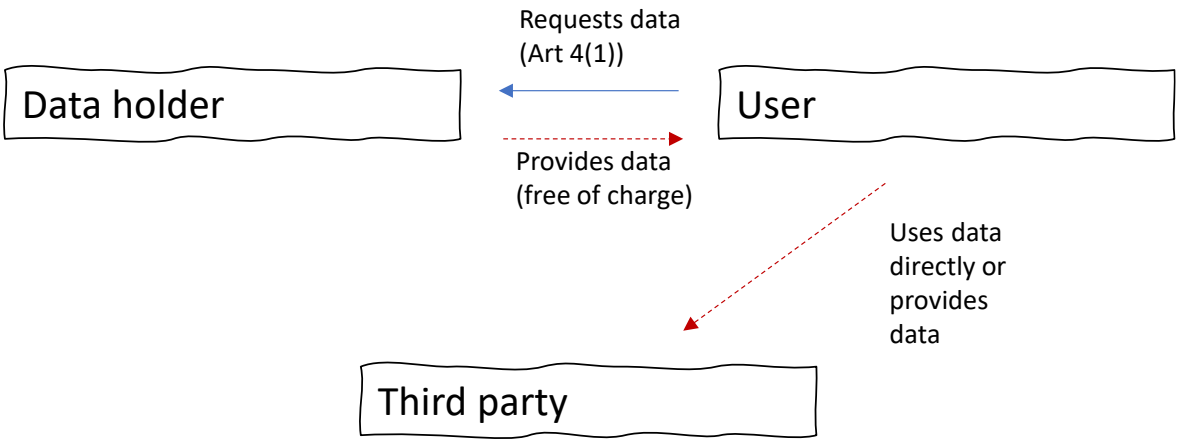
The result is that for any situation in which data sharing is costly for the data holder, the user will pay at least part of the cost, while the incentives for the data holder to optimise its sharing infrastructure are seriously distorted.

*Recommendation: data holders should have the right to fair and reasonable compensation for any data sharing, including with users.*




[25] Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Data Act, Available: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Position_Statement_MPI_Data_Act_Formal__13.06.2022.pdf

In additional, there is a potential for serious conflict between the user right to request data holders to make user data available to third parties (Art 5(1)) and the requirement that data recipients agree FRAND terms for the transfer of user data (Art 8(1), (2)) in cases where there is a dispute about the FRAND terms between the recipient and the data holder. As the Max Planck Institute (p. 28) points out "allowing the data holder to retain the data until the FRAND dispute is resolved would lead to a violation of the obligation of the data holder vis-à-vis the user and seriously affect the effectiveness of the data access and use right of the latter.[26] Conversely, if one considers the data holder under an obligation to provide access despite its failure to agree on FRAND terms, this would create a so-called 'hold-out' situation, where the third party can simply refuse or evade honest FRAND negotiations, as this will not hinder the provision of the service. Even more, one may wonder what the third party must pay for if the data will anyhow have to be made available to the third party pursuant to Article 5(1)."




Finally, the ability of users to transfer data received as a result to an Art 4(1) request to a third party at a later stage undermines the protection of the data holder from harm arising from data use by the third party given by the right to agree compensation and impose conditions where they are obliged to give third parties direct access to user data.[27]

## 2.3 Risks and opportunities derived from the Data Act

This section describes the risks and opportunities that may arise from the B2C and B2B data sharing obligations in the Data Act. The section is based on the points raised during stakeholder interviews with ETNO members, as well as responses to the survey.[28]

### 2.3.1 Risks identified in stakeholder interviews

**Legal risks of ensuring that data is compliant with GDPR**

To remain compliant with GDPR, data providers **must ensure that data is non-personal, or that consent is obtained from data subject** before sharing it with other businesses or consumers. This incurs legal costs on the provider as data will have to be checked and verified, possibly requiring

[26] Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Data Act, Available: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Position_Statement_MPI_Data_Act_Formal__13.06.2022.pdf

[27] European Commission (2022) Commission Staff Working Document – Impact Assessment Report. (Annex 8. P. 145) Available at https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act

[28] Interview guide and survey can be found in **Annex 1** and **Annex 2** respectively.

input from a legal professional. The Data Act is not clear on who will bear these costs but if it falls to the data provider, B2B/B2C data sharing will be a costly process and the obligation to share data becomes unfair. Given the nature of data collected by telecom companies it is difficult to distinguish what constitutes personal and non-personal data. The Data Act would therefore have a disproportionate impact on these companies.

This risk arises if the Data Act is to be **overruled by other legislation such as GDPR** because the examination of datasets would have to ensure that personal data is anonymised or otherwise made compliant prior to sharing with third parties. If this process is not thorough, the data provider is exposed to legal and reputational risk.

**Risk of liability if data is misinterpreted, lost, or misused**

The B2B and B2C aspects of data sharing expose data providers to risk if data is **misinterpreted, lost, or used by data recipients for nefarious purposes** and the Data Act does not indicate who is liable if this were to happen. These issues may be avoided if the provider works alongside the data recipient to navigate and draw insights from the information, but this will enhance the burden on data providers. Furthermore, if the data has been processed by the provider, it may increase the risk of liability for misinterpretation. This **exposes the data provider to additional liability risks**.

**Costs associated with making data available B2B and B2C**

Under the Data Act, data holders must provide relevant data to customers and other businesses upon request. Companies may need to build Application Programming Interfaces (APIs) to allow third parties access to data collected from IoT devices. This would require resources not only for **building the API**, but also for the **maintenance**. There are also **security risks** associated with having a backdoor to such data lakes.

In addition to the direct costs of building interfaces to extract and share data, there are also **opportunity costs** for businesses. The time and resources spent by data holders on fulfilling the obligations set out in the Data Act cannot be used for other purposes such as business development or innovation.

For B2C and B2B data sharing, it is not straightforward or without expense to extract data from devices on demand. This is not currently accounted for appropriately in the Data Act.

**Lack of protection for related services is a disincentive for developing new service solutions**

Article 6 of the Data Act mentions some protective measures for intellectual property concerning products but **does not outline the same measures for related services**. For businesses who have invested in developing services and who have built their business on these services, there is a notable disadvantage. For example, if a company has spent years developing tailored smart home applications, and they are obliged through the Data Act to share this service data, a competitor could use the data to build similar applications. If this is the case, **companies will be deterred from investing in related services and innovation will be negatively impacted**.

If there is to be obligatory data sharing, particularly on a B2B level, ETNO members would like the Data Act to **provide the same level of protection for related services as is granted to the manufacturers of connected products**. It would be unfair if data were used by a third-party organisation for the development of a service that stands in direct competition with the service from which the data was originally obtained from. Granting the same level of protections for manufacturers and service providers would support the objective of the Data Act to facilitate after-

market competition, by enabling data access for the development of new and innovative products and services, while protecting data holders from unfair competition.

**Safeguards must be defended to prevent gatekeeper power from being reinforced in the market**

There is a risk that obligatory B2B data sharing will reinforce gatekeeper power in the market. Although the regulation promises that gatekeepers will not benefit from B2B data sharing, it is **difficult to keep these powerful companies from finding loopholes in the system**. Gatekeepers may get access to data from smaller organisations and use it to expand business, develop new products/solutions and increase their already dominant share in the market. If the Data Act cannot successfully prevent dominant players from benefiting from the new legislation, this could **damage healthy competition in the market and limit opportunities for smaller firms**.

### 2.3.2 Potential opportunities identified in stakeholder interviews

**Opening other markets**

The Data Act will open markets where limited data access has previously been a barrier to entry. For example, the electric metering market is currently closed off as the only company that can provide services related to metering products is the distributer. If the Data Act made data sharing mandatory on a B2B scale, there is an opportunity for telecom operators to obtain data from the distributer and use it to build new services, for example, this could allow telecoms to **expand into the electric metering market.** The **connected car market** is another market that could be accessed by telecoms under the Data Act. There are many devices interacting within this market and with free access to data from other players, telecoms could expand business into this market. The Data Act and B2B data sharing, therefore, offer telecoms a **route into other markets** and, in turn, a way to increase their portfolio of related services and/or products.

Because the Data Act creates a legal obligation for businesses to share data, it could create new markets for data. Some telecom operators mentioned that this could create an opportunity for them to become **data intermediaries/brokers**, or to provide a marketplace for data to be traded.

**Standardising APIs allows for the integration of various smart devices**

B2B data sharing under the Data Act **provides an incentive for companies to standardise APIs** and there would be an **opportunity for telecoms to integrate a variety of smart devices**, for example, it would allow one dashboard to be created for all smart city devices. Telecom companies could then incorporate more products into related services that they offer and increase the value of these services. This will have knock-on benefits for the public as related services will provide more information, be more efficient and possibly be quicker to establish. This benefit would be brought about by the Data Act's vision for a single data market and encouraging data sharing on a B2B level.

## 2.4 Overall impacts of the B2C and B2B data sharing obligations

The following table illustrates the potential impact of the Data Act on each of the business models discussed in this section. The first column indicates the relative importance of each business model to ETNO members, while the second denotes the degree of impact the Data Act may have on each model. The level of uncertainty in the degree of impact is also indicated, as in various cases there is some ambiguity in the scope of the Data Act.

These indicative parameters were derived from interviews with ETNO members, responses to questionnaires submitted to ETNO members, and desk research. Note that the parameters

represent a synthesis of our findings and do not necessarily reflect the business of any individual ETNO member.

**Table 1 Summary of the impact of the B2C and B2B data sharing obligations**

| Business model | Importance of business model to telecom operators | Impact of the Data Act on the business model | Level of uncertainty | Notes |
|---|---|---|---|---|
| 1A: Only connectivity supplied by telecom operators | ● | ●* | ????? | The impact depends on the extent to which ECS data fall within the scope of the Data Act. |
| 1B: related services provided by telecom operator; hardware supplied by 3rd party | ◕ | ◑ | ???? | Telecom operator may be the data holder in this scenario, depending on the context and nature of the services supplied. Some new data requests may be directed at other entities, lessening the impact on operators relative to 1D. |
| 1C: services/ management layer provided by 3rd party, hardware and connectivity supplied by telecom operator | ◑ | ○ | ???? | It is unlikely that telecom operators would be considered the data holder as in many cases they will not hold or have access to data generated by connected devices. |
| 1D: hardware and related services supplied by telecom operator | ◕ | ◕ | ??? | Telecom operator is the data holder in this scenario. However, it is unclear how many new requests there would be. |

Notes: ○◔◑ ◕ ● denote impact from low to high. ? - ????? denotes low to high uncertainty about the potential impact.

* denotes degree of impact if ECS are fully within scope of the Data Act.

Note that business model 1A presents the greatest degree of ambiguity in the analysis. It is evident that providing IoT connectivity is an important business model for ETNO members and the issue of whether ECS data are in scope or not is key.

# 3 B2G data sharing provisions

This section describes ETNO members' business models that are likely to be most heavily impacted by chapter V of the Data Act. It is informed by interviews with ETNO members, desk research and analysis of the draft Data Act.

Chapter V of the Act (Articles 14-22) sets out obligations for making data available to public sector institutions demonstrating an 'exceptional need' to use the data requested. An exceptional need is deemed to exist in the following circumstances (Article 15):

a) *where the data requested is necessary to respond to a public emergency;*

b) *where the data request is limited in time and scope and necessary to prevent a public emergency or to assist the recovery from a public emergency;*

c) *where the lack of available data prevents the public sector body or Union institution, agency, or body from fulfilling a specific task in the public interest that has been explicitly provided by law; and*

   i) *the public sector body or Union institution, agency or body has been unable to obtain such data by alternative means, including by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data; or*

   ii) *obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders or other enterprises.*

These provisions appear to cover any type of data held by telecom operators, unless they are small or micro enterprises – provided the exceptional need criteria are met. Any operator business model that generates data of any sort would therefore potentially be in the scope of the B2G data sharing provisions of the Act.

### Box 6 Recommendations regarding B2G data sharing provisions

**The definition of concepts such as "public emergency" and "exceptional need for data" need to be clarified and circumscribed**. Access obligations, as a measure of last resort, should be limited to clearly specified cases of truly exceptional nature (e.g., officially declared public emergencies).

The Data Act also needs to clarify that any data provided to public sector bodies cannot be used for purposes other than the one for which it is requested.

The Data Act should **recognise that adequate compensation is required** to incentivise ongoing investment in data infrastructures. The process of preparing data to high-quality standards is costly regardless of the reason motivating the data request. The current proposal can lead to a situation in which governments interpret broadly what a 'public emergency' is to put forward data requests under Article 15(a) and data controllers share incoherent datasets (that governments will not have the required skillsets to handle) of a subpar quality to cut costs since they're not entitled to compensation.

## 3.1 Case studies of affected business models

TIM, A1 Telekom Austria Group, Deutsche Telekom, and Telefónica provided information about the data they share with public sector organisations under specific contracts. This section presents case studies of the data sharing arrangements that they described, grouped into three categories: Mobility insights, the Covid-19 pandemic, and Data sharing with National statistics institutes.

1) Mobility insights

- **Telefónica** reported two types of services in this area:
  - Delivery of tourism insights to local authorities (on standard commercial terms): an example of such service is a recent project in which Telefonica helped municipalities in the Barcelona Metropolitan area to analyse the profiles of their tourists (including where they come from, what offer they have chosen, how much they have spent and consumed), to improve the touristic offer. In particular, they offered a dashboard that puts together anonymised and aggregated data from Telefonica mobile network, credit card transactions, flight and hotel booking, and data from the Internet and social media. This service is supplied as an alternative to more traditional solutions for tourist profiling like surveys.
  - Provision of origin/destination matrices to public transport authorities and companies (on standard commercial terms): Telefonica provides Highways England with its anonymised database containing over four billion network events generated every day by O2 customers. This data, together with the data collected by the road operator, is used by Highway England to improve their infrastructure modelling and planning and simplify processes.
- **Deutsche Telekom's** fully owned subsidiary T-Systems supplies mobility insights via its unit called 'Motion Data'. Through this unit, T-Systems analyses movement, and traffic flows, e.g., in pedestrian zones, on the road or in local traffic, based on anonymised signalling data from the mobile network of Deutsche Telekom. These data can then be used for different applications, from traffic planning to marketing actions.
- **TIM** and **A1 Telekom Austria Group** also offer solutions in the field of mobility data, which they call, respectively *Presence and Mobility Data for tourism, safety and city management* and *Mobility Insights solutions*. These are provided to public sector organisations, on an aggregated and anonymised basis in compliance with GDPR, and standard commercial terms.
- **Orange** offers a service called *Flux Vision*, through which they supply statistic indicators of attendance, patterns of movements and segmentation information based on data from the Orange mobile network. Data are irreversibly anonymized and are offered as solutions for the public sector in the context of:
  - Transport: Adapt infrastructure size or services according to passengers' movements;
  - Tourism/Events: Analyse seasonality flows and the impacts of events.
- **Proximus** offers solutions to public sector organisations through *Proximus analytics* for:
  - Traffic management: monitoring of traffic flows in real-time based on the combined data of road segments and people's mobility behaviour, by combining historical positions of connected vehicles with data from sensors along the road or at car parks;
  - Crowd management: monitoring the group formation, movements, and disbursement during a specific time window of an activity/event to allow authorities to react quicker and more efficiently to situations.
- **Telia** offers a service called *Crowd Insights*, applicable to:

- Municipalities to measure the volume of people and compare activity levels between locations – or the same location on different days; this information can be used, for instance, to grasp which areas have the most activity at the weekends and during the week and which need more public services.
- Events and Tourism: to get the profile of tourists, what they do when they come to town, how long they stay if they come for an event, seasonal, weekly, and daily trends, and places visitors tend not to go.
- Transport: through crowd movement patterns Telia offers information on where people start and end their journeys and their routes, which can be used to understand what passengers want and therefore offer a better service.

2) Covid-19 pandemic

- **TIM, Deutsche Telekom, Telefonica, Vodafone, and Oranges** alongside several other European telecom operators in 2020 and 2021 provided the JRC of the European Commission with anonymised data about people's movement from/to destinations during the pandemic. This was realised in the context of the Data4Covid project, in which telecom operators shared aggregated and anonymised data in compliance with GDPR to help and support the JRC and the EU Commission to monitor lockdown situations.
- **Telefonica** during the first wave of the pandemic provided the ONS with real-time mobility data to get insights into public compliance in response to the mobility restrictions imposed. In addition, it informed the government decision-making on the next steps to help curb the spread of COVID-19 in the UK.

3) National statistics institutes

- **Telefonica** is working with the Spanish National Institute of Statistics to complement their traditional data collection model (based 100% on surveys) with data from Telefónica's mobile network, among others, to provide society with much more frequent, detailed, and timely information. This project is provided on standard commercial terms.
- **Deutsche Telekom** provided, together with Telefonica Deutschland, the German Federal Statistical Office with mobile phone network data to allow them to compare the two datasets, examine the presence of skews and distortions, and assess the usability of mobile phone data for official statistics in various feasibility studies.

## 3.2 Impact of B2G data sharing provisions

The ambiguities in the Act make it difficult to estimate what impact the B2G data sharing provisions will have on telecom operators. In particular, the circumstances under which data can be requested by the public sector, the ultimate use of that data and the type of data that can be requested are still unclear. There is also a need to clarify how the Data Act will interact with GDPR.

As mentioned by the European Commission Regulatory Scrutiny Board and in the French Presidency Progress Report[29], **the concept of 'exceptional need to use data' is too vague and should leave less room for (mis)interpretation**. Article 15 provides circumstances to be considered in that situation that are unclear and gives public sector bodies large room for interpretation, especially point (c).

Article 15(c)(1) sets some requirements for mandatory access in non-emergency cases, including that the public sector body puts a reasonable effort in trying to obtain the data at market rates. The Max Planck Institute argues that Recital 58 should include a reference to the cost-based approach

[29] French Presidency Progress Report on the Data Act, 16 May 2022

described in Article 20(2) to determine whether the price matches market rates.[30] Also, Article 15 should be interpreted as a means to request ad hoc access only.

The requirement that new legislation could not ensure the timely availability of the data is vague and could potentially lead to a deadlock if Member States are pre-empted from legislating on issues covered by the Data Act, while at the same time attempting to enact legislation is a prerequisite for the legitimacy of requests under Article 15(c)(1).

Article 15(c)(2) could at best allow only one-off requests, but the possibility that the public sector body could mandate data access under Chapter V even if it could obtain the data in other ways in cases where that 'would substantially reduce the administrative burden for data holders or other enterprises' is logically flawed and contradicts Article 15(c), 1st sentence.

Broad and vague requests from the public sector are wholly unsuitable, and legal certainty is needed on when data requests are lawful to avoid any risk of potential misuse and/or unlawful sharing of data. Data requests should be specific and proportionate and public authorities need to consider that in some instances data requested may not be available from the industry or suitable in the format requested. By way of example, it may not be appropriate for a public authority to ask for a raw dataset which contains data going beyond the purpose required where a subset of the data could be extracted for the purpose required.

On Article 19 of the Data Act there are **concerns about how public bodies might use data** received under Article 14. Public sector bodies should "*not use the data in a manner incompatible with the purpose for which they were requested.*" This incompatibility test could have the effect of broadening the purpose beyond what was originally stated. It is unclear why the purpose could not be limited to the explicitly requested purpose.

It should also be noted that there is **no requirement to have in place a data-sharing agreement** with a public sector body following a request for data. It would be unusual practice for a private organisation to share personal data under the GDPR with a public sector body with no contractual arrangement governing the sharing, including provisions relating to deletion, security, minimisation, and purpose. A similar arrangement should be considered here.

## 3.3 Risks and opportunities derived from the Data Act

This section describes the risks and opportunities that may arise from the B2G data sharing obligations in the Data Act (Chapter V). The section is based on the points raised during stakeholder interviews with ETNO members, as well as responses to the survey.[31]

### 3.3.1 Risks identified in stakeholder interviews

**Cost of converting raw data into insightful data for B2G**

There are **direct financial costs involved in converting raw data into insightful data**, including any necessary software/hardware investments and the cost of labour. Depending on the size of the dataset, storage costs may also be incurred by collecting and holding data during conversion. If these costs are born by the telecom operator and no compensation is offered by governments, they are a

[30] Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Data Act, Available: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Position_Statement_MPI_Data_Act_Formal__13.06.2022.pdf

[31] Interview guide and survey can be found in **Annex 1** and **Annex 2** respectively.

burden on the telecom company. To minimise these costs, telecom operators run the risk of **jeopardising data quality.**

The Data Act does not sufficiently acknowledge such costs or address how companies will be compensated for the data preparation process. If insightful datasets are required by public bodies in 'emergency' cases, then compensation would make the data obligation more effective. Otherwise, ETNO members prefer that data provision is done on a voluntary basis as it currently is.

**Opportunity cost of allocating resources to B2G data preparation**

Data cannot be provided to third parties without a certain level of preparation. To be insightful, raw data must be cleaned, processed, and interpreted. In some cases, **raw datasets are extremely complex**, and it will require much **time and resources to ensure the quality of the data** is fit for purpose. EU telecom operators fear that governments will not have the required skillsets to handle this preparation and as such, it falls on the data provider to carry out the heavy lifting on data preparation. It is also a concern that governments don't always know which data they need, and that telecom operators will have to spend time understanding their needs to tell them which datasets will be useful.

This is an **opportunity cost** for the telecom as these resources could otherwise be employed more productively in the company. For example, if a government requests a dataset from a telecom that is complex and significantly unrefined, it may take the telecom operator's top data scientist a year to process this dataset. During this time, the company is losing out on an expert skillset which may otherwise be used for business development purposes.

It is **not practical for governments to accept unprocessed data,** especially in the case of emergencies where they would need insightful data to make prompt decisions. The effort required to meet the B2G demands of the Data Act could tie up important resources, in terms of labour, capital and time, for telecom operators.

**Legal risks of ensuring that data is non-personal**

To remain compliant with GDPR, data providers **must ensure that individuals are not identifiable before sharing it with government bodies**. This incurs **legal costs** on the provider as data will have to be checked and verified, possibly requiring input from a legal professional. The Data Act is not clear on who will bear these costs but if it falls on the data provider, B2G data sharing will be a costly process and the obligation to share data becomes unfair. Given the sensitive nature of the data collected by telecom operators (such as location data) as well as the sheer volume of data collected, having to anonymise/pseudonymise data has a disproportionate impact on these companies.

This risk arises if **the Data Act is to be overruled by other legislation** such as the eprivacy regulation and GDPR as the examination of datasets will have to ensure that individuals are not identifiable prior to sharing with governments. If this process is not thorough, the data provider is exposed to legal risk.

**Risk of liability if data is misinterpreted / lost**

There is a risk when companies provide data to governments that this data will be **misinterpreted, lost, or compromised** (for example if it was shared with unauthorised third parties). Under the Data Act, it is not clear whether **the data holder or the recipient will be liable** if this were to happen. Misinterpretations may be avoided if the holder works in tandem with the data recipient to navigate and draw insights from the information, but this will only enhance the burden on the data holder by increasing preparation demands. Alternatively, the Data Act could explicitly assign responsibility to

the data recipient for secure handling of the data. Furthermore, if the data is well-refined by the data holder before handing it over to government, will the holder be more liable for a misinterpretation? This **exposes the data holder to liability risks**.

The B2G aspect of data sharing leaves data holders open to risk and the Data Act is not clear on procedures regarding data misinterpretation and liability.

**Risk of 'public emergency' being defined too broadly**

If the definitions of "public emergency" and "exceptional need" in the Data Act are too broad, there is a risk that **governments could take advantage** of these obligation and place a higher demand on telecom operators to provide data. Without compensation, this could result in low-quality data and poor processing as companies try to cut costs. Furthermore, the lack of compensation will undermine telecom operators' incentives to design innovative data services which could add real value to the public sector.

Without a clear definition, different jurisdictions may also declare emergencies at different times which may present challenges to companies that operate in multiple markets. A **lack of distinction between emergency prevention, emergency response and emergency recovery** are also a concern. This could lead to a situation where telecom operators start providing data on a regular basis without a clearly defined endpoint.

## 3.4 Overall impacts of the B2G data sharing obligations

**Table 2 Summary of the impact of the B2G data sharing obligations**

| Business model | Degree of impact | Level of uncertainty | Notes |
|---|---|---|---|
| 2: All models affected by B2G data sharing provisions | ● | ?? | Any operator business model that generates data of any sort is potentially in scope of the Act. |

Notes: ○◔◑◕● denote impact from low to high. ? - ????? denotes low to high uncertainty about the potential impact.

# 4 Data processing service switching obligations

The Data Act aims to remove obstacles to effective switching between providers of data processing services, including cloud and edge services. In this context, a data processing service is defined as:

> *"a digital service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature"*

Its provisions include (Articles 23-26):

- a mandatory maximum switching period of 30 days;
- requiring the service provider to assist in the switching process;
- reducing allowable switching charges; and
- ensuring the customer enjoys "functional equivalence" in the use of the new service.

**Box 7 Recommendations regarding the data processing service switching obligations**

The Data Act should **clarify who is responsible for the switching process in multi-party business models** and ensure that resellers, who are simply reselling a cloud service offered by a third-party, have a legal claim vis-à-vis said third-party to ensure the effective implementation of switching requirements for their customers.

The Act should be modified so that cloud service providers and their enterprise customers can **agree on a different notice and switching period,** in particular if this benefits the customer.

## 4.1 Affected business models

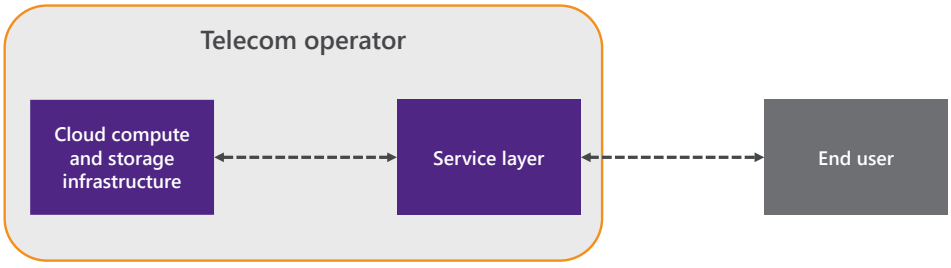
This affects a number of business models offered by telecom operators, including cloud computing services accessed over a network and edge computing services (where data are processed and/or stored close to where they are generated).

### 4.1.1 Telecom operators as cloud service and infrastructure suppliers

The first identified business model in this area is one where an operator supplies both the cloud infrastructure and the service layer and manages the customer relationship. In this case, switching obligations would be borne by the operator.

We understand that this business model is only offered by a subset of ETNO members, with reselling or acting as Managed Service Provider (MSP) being the more common. Nevertheless, for some operators this represents an important business model.

**Figure 7 Business Model 3A - Telecom operators as cloud service and infrastructure suppliers**

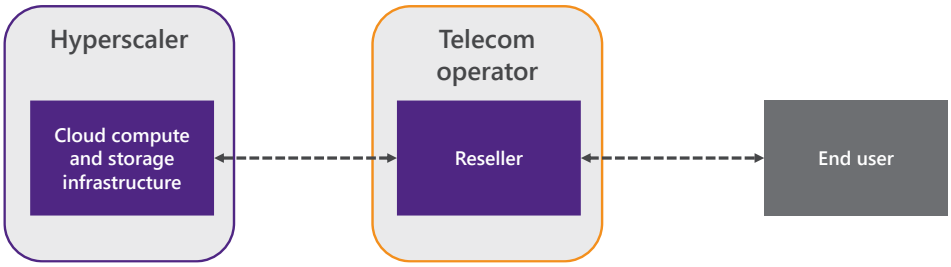


### 4.1.2 Telecom operators as resellers of 3rd party cloud services

Another business model involves the resale of 3rd party cloud services – generally, those offered by hyperscale cloud providers (AWS, Google Cloud and Microsoft Azure).

In this situation, the end-user has a contractual agreement with the telecom operator, which acts legally as the cloud provider. The telecom operator therefore would be subject to the provisions under the Act that relate to data processing service switching. The telecom operator also has a contractual relationship with the cloud supplier but, as it is not the customer, would not appear to be able to exercise the same rights as customers under the Act.

**Figure 8 Business Model 3B - Telecom operators as resellers of 3rd party cloud services**

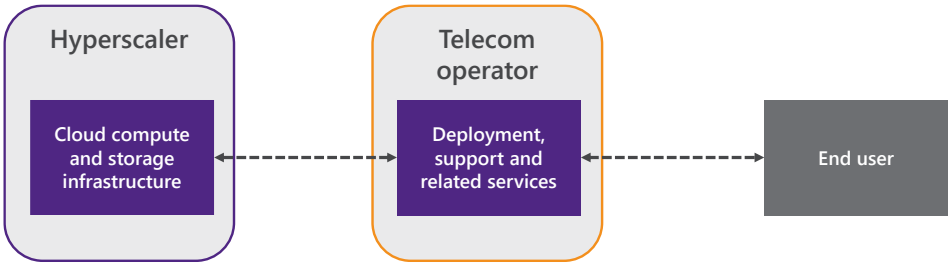



### 4.1.3 Telecom operators as Managed Service Providers (MSPs) of 3rd party cloud services

This model is similar to the reseller model, but the cloud service is part of a broader service package which may include deployment, optimisation, IT support, cybersecurity and applications.

In this situation, the end user (typically an enterprise user) has a contractual agreement with the telecom operator, which acts legally as the cloud provider. The telecom operator would be subject to most of the switching provisions under the Act that relate to end-user switching. The telecom operator also has a contractual relationship with the cloud supplier but, as it is not the customer, would not appear to be subject to the same provisions under the Act.

**Figure 9 Business Model 3C - Telecom operators as MSPs of 3rd party cloud services**

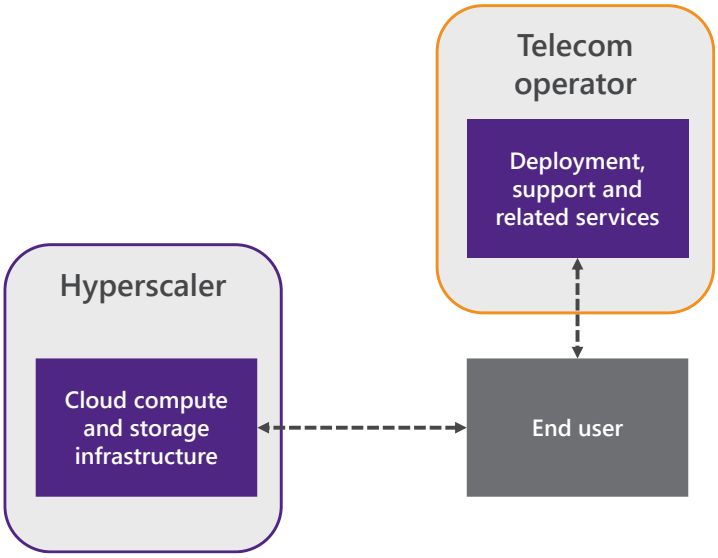



### 4.1.4 Telecom operators as Managed Service Providers (MSPs) only of 3rd party cloud services

In this business model the telecom operator acts as MSP (without re-selling), providing services which may include deployment, optimisation, IT support, cybersecurity, and applications.

It is not clear whether such services fall under the definition of a 'data processing service' in the Data Act. As per Article 2(12), *'data processing service' means a digital service […], provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature".* The extent to which this definition covers managed services in instances where the telecom operator is not the reseller is likely to depend on the context and nature of the services supplied.

**Figure 10 Business model 3D – Telecom operators as MSPs (only) of 3rd party cloud services**




### 4.1.5 Telecom operators as consumers of data processing services

It should also be noted that telecom operators are themselves consumers of data processing services to enhance and improve their own business efficiency. As customers, they would be able to benefit from the switching provisions of the Data Act.

## 4.2 Impact of Data processing service switching obligations

**Switching and portability processes should be proportionate to the technical complexity.** The obligation to include a contractual requirement imposing a maximum notice period of 30 calendar days for terminating a contract could be unfeasible for more complex or customized cloud projects and may require significant upfront investments. To properly balance this with the customer's right to switch, we suggest to carefully evaluate the introduction of a short notice period against the possibility of the provider and the customer to mutually agree on long-term contractual commitments in a B2B environment.

In practice a longer period than 30-calendar days may be reasonably required in certain well-defined circumstances. Several different parties may also need to be involved to enable a switch if complex business models are involved in the delivery of digital services of this nature. While the Act does allow for complaints to be made to national authorities (See Art 32) for infringements of its provisions and penalties (Art 33), this matter is better left to contracting parties to negotiate, as different business models and contexts may have differing timing challenges (provided that both parties can influence the content of such a provision).

## 4.3 Risks and opportunities derived from the Data Act

Chapter VI of the Data Act proposal aims at facilitating the switching of cloud services to enable customers to move from one provider to another and make the market of data processing services more competitive and increase the degree of interoperability across different providers. This will ensure that data can be shared easily within and across sectoral ecosystems. The objective of the new rules on switching is to address lock-in effects in the cloud market to increase choice for business users and individuals of data processing services. This will be achieved by requiring cloud providers to remove commercial, technical, contractual, and organisational obstacles to switching.[32]

The proposal includes a provision to guarantee that customers should maintain functional equivalence of the service after the transition to an alternative supplier. The Data Act includes an exception for technical unfeasibility but puts the burden of proof on the service provider. The proposal does not mandate specific technical standards or interfaces. However, it requires services to be compatible with European standards or open interoperability technical specifications where these exist.

### 4.3.1 Risks identified in stakeholder interviews

**Adhering to the 30-day switching period**

While supporting the goal to facilitate cloud switching, ETNO members do not feel that switching providers can be always done efficiently within a 30-day time frame. While this time frame should be sufficient for many B2C process and IaaS services, in certain customer-specific cases, **switching would require rebuilding infrastructure and redesigning hardware**, especially where cloud and edge solutions are bespoke. The Data Act addresses contractual, commercial, and organisational barriers to switching but **does not consider the logistical difficulties involved in some switching processes.**

Moreover, the Data Act is not clear enough when it comes to more complex contractual situations, e.g., where a telecom operator acts as a re-seller of a cloud service that is provided by a different entity – referred to here as the technology provider. In such a constellation, the telecom operator would hold the contractual relationship over this cloud service with the customer but is itself rather a partner than a customer of the provider of the underlying cloud platform. This might result in an implementation gap where the customer invokes his right to switch vis-à-vis the contractual partner, i.e., the telecom operator, but the latter has no legal claim towards the technology provider who controls the technical design of the platform. To solve this and to ensure proper enforcement of switching rules, resellers, and technology partners (e.g., managed service providers) would need to have a legal claim against the cloud technology provider even though they are themselves not a customer.

### 4.3.2 Potential opportunities identified in stakeholder interviews

The Data Act is intended to facilitate switching between cloud and edge services providers that cover the same type of services. For telecom operators who are **customers of cloud services, easier**

[32] Linklaters, EU: The "Data Act" – New rules on IoT data and switching cloud services, March 2022. https://www.linklaters.com/en/insights/blogs/digilinks/2022/march/eu---the-data-act---new-rules-on-iot-data-and-switching-cloud-services#:~:text=The%20objectives%20of%20the%20Data%20Act%20%E2%80%93%20Cloud%20switching,technical%2C%20contractual%20and%20organisational%20obstacles .

**switching between providers is beneficial**. The Data Act will allow telecoms more flexibility to switch to providers with lower costs, higher levels of security, or to meet changing business needs.

Currently, the process of switching is complicated, involving obstacles of commercial, technical, contractual, and organisational natures that inhibit users from switching to another provider of the same type of service.[33, 34] The Data Act requires such obstacles to be removed, allowing telecoms and other organisations to switch cloud providers with ease, and allowing telecom operators acting as MSPs to support switching processes for their customers.

## 4.4 Overall impacts of the Data Processing service switching obligations

**Table 3 Summary of the impact of the Data Processing service switching obligations**

| Business model | Importance of business model to telecom operators | Impact of the Data Act on the business model | Level of uncertainty | Notes |
|---|---|---|---|---|
| 3A: Telecom operators as cloud suppliers using their own infrastructure | ● | ◕ | ??? | Only certain operators provide their own cloud infrastructure, but many offer edge computing type services. Edge deployment generally involves the deployment of hardware, raising the risk of stranded assets. |
| 3B: Telecom operators as resellers of third-party cloud services | ◕ | ◑ | ??? | The telecom operator acts legally as the cloud provider in such cases, and would likely incur some administrative burden in facilitating switching. |
| 3C: Telecom operators as resellers and Managed Service Providers (MSPs) of third-party cloud services | ◕ | ◑ | ??? | The telecom operator acts legally as the cloud provider in such cases and would likely incur some administrative burden in facilitating switching. |
| 3D: Telecom operators as Managed Service Providers (MSPs) of third-party cloud services without reselling. | ◑ | ◔ | ???? | It is not clear whether the Data Act considers pure Managed Service Provision as constituting a Data Processing Service. |

[33] LinkLater, "EU: The "Data Act" – New rules on IoT data and switching cloud services" found at https://www.linklaters.com/en/insights/blogs/digilinks/2022/march/eu---the-data-act---new-rules-on-iot-data-and-switching-cloud-services

[34] Authority for Consumer & Markets, "Market study into cloud services" found at https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf

| Business model | Importance of business model to telecom operators | Impact of the Data Act on the business model | Level of uncertainty | Notes |
|---|---|---|---|---|
| 3E: Telecom operators as consumers of cloud services | ● | ◑ | ??? | Telecom operators may take advantage of the switching provisions themselves, however it appears unlikely that they would regularly switch. |

Notes: ○◔◑◕● denote impact from low to high. ? - ????? denotes low to high uncertainty about the potential impact.

# 5 Summary of the impact of the Data Act on telecom operators

**Table 4 Summary of the impact of the Data Act**

| Business model | Importance of business model to telecom operators | Impact of the Data Act on the business model | Level of uncertainty | Notes |
|---|---|---|---|---|
| 1A: Only connectivity supplied by telecom operators | ● | ●* | ????? | The impact depends on the extent to which ECS data fall within the scope of the Data Act. |
| 1B: related services provided by telecom operator; hardware supplied by 3rd party | ◕ | ◑ | ???? | Telecom operator may be the data holder in this scenario, depending on the context and nature of the services supplied. Some new data requests may be directed at other entities, lessening the impact on operators relative to 1D. |
| 1C: services/ management layer provided by 3rd party, hardware and connectivity supplied by telecom operator | ◑ | ○ | ???? | It is unlikely that telecom operators would be considered the data holder as in many cases they will not hold or have access to data generated by connected devices. |
| 1D: hardware and related services supplied by telecom operator | ◕ | ◕ | ??? | Telecom operator is the data holder in this scenario. However, it is unclear how many new requests there would be. |
| | | | | |
| 3A: Telecom operators as cloud suppliers using their own infrastructure | ● | ◕ | ??? | Only certain operators provide their own cloud infrastructure, but many offer edge computing type services. Edge deployment generally involves the deployment of hardware, raising the risk of stranded assets. |
| 3B: Telecom operators as resellers of third-party cloud services | ◕ | ◑ | ??? | The telecom operator acts legally as the cloud provider in such cases and would likely incur some administrative burden in facilitating switching. |
| 3C: Telecom operators as resellers and Managed Service Providers (MSPs) of third-party cloud services | ◕ | ◑ | ??? | The telecom operator acts legally as the cloud provider in such cases and would likely incur some administrative burden in facilitating switching. |

| Business model | Importance of business model to telecom operators | Impact of the Data Act on the business model | Level of uncertainty | Notes |
|---|---|---|---|---|
| 3D: Telecom operators as Managed Service Providers (MSPs) of third-party cloud services without reselling. | ◑ | ◔ | ???? | It is not clear whether the Data Act considers pure Managed Service Provision as constituting a Data Processing Service. |
| 3E: Telecom operators as consumers of cloud services | ● | ◑ | ??? | Telecom operators may take advantage of the switching provisions themselves, however it appears unlikely that they would regularly switch. |

Notes: ○◔◑◕● denote impact from low to high. ? - ????? denotes low to high uncertainty about the potential impact.

Interview participants raised concerns about **the scope of the Data Act** and which products and services would be affected. The definitions of "IoT devices", "virtual assistants" and "related services" need clarity and to explicitly outline what products/ services are included and excluded. The scope of these definitions will have a substantial effect on how the Data Act will impact telecom operators. In particular, from the current phrasing of the proposal, it is assumed that Electronic Communication Service (ECS) data, such as metadata and content of communications data, will be excluded based on the fact that ECS cannot be regarded as a "related service". This is important, as including ECS data would dramatically increase the impact that the Data Act could have on telecom operators.

Another concern is that B2B, B2C and B2G data sharing will incur significant **legal costs to the data holder**. Ensuring that GDPR requirements are met before data is shared with a third party may be costly both in terms of time and resources where data is personal. For example, where data is personal, the data holder may need to ensure that consent is obtained or that data are anonymised. This makes it difficult, as well as expensive, for data providers to respond to data requests. If this verification is not done correctly, the data provider is exposed to legal risk and further legal costs. If data recipients lose or misinterpret the data, again there is a risk that data holders will face legal consequences and additional costs.

Some stakeholders also identified opportunities that may arise from the Data Act for telecom companies. B2B and B2C data sharing will facilitate the integration of various IoT devices, allowing telecoms to improve current offerings and build new business. Other markets, where data access had previously been a barrier to entry, could be opened by the Data Act. If the Data Act can facilitate a larger market for data, there may also be an opportunity for telecom operators to become data intermediaries, or to expand on the broker services that they offer.[35]

The main concerns for the stakeholders that were interviewed are with **B2G data sharing** and the direct and indirect costs of providing governments with data. ETNO members feel that the process of preparing data is being overlooked by the legislation and that this cannot be done to a high quality without compensation, particularly if "public emergency" is interpreted too broadly. To cut costs, data preparation will be of subpar quality and a lose-lose situation arises whereby governments are

[35] For example, Deutsche Telekom created the Data Intelligence Hub, which is a marketplace for data.

receiving incoherent datasets that they do not have the skill set to interpret. Interview participants indicated that a requirement that would effectively force the data holder to make data available without fair compensation is undesirable for both telecom operators and public bodies.

Regarding **Cloud and Edge Services**, the impacts are still unclear as the legislation does not specify who is responsible for this switching process in multi-party business models, in particular involving re-sellers. A second concern is the feasibility of switching service providers within a 30-day period as suggested in the Data Act may be unrealistic in some cases. Some cloud offerings are customised for businesses and may be highly bespoke depending on the size of the organisations and flexibility is desirable in those cases. Furthermore, switching providers may involve a reconstruction of hardware in the case of bespoke edge computing.

# 6 Conclusion

## 6.1 B2C and B2B data sharing provisions

The Data Act proposals are intended to tackle "the insufficient availability of data for use and reuse in the European economy or for societal purposes".[36] Consequently, the proposals include access and use rights to overcome lock-in, enable innovation and prevent data holders from retaining data for the sole purpose of technically tying aftermarket services to IoT products.[37]

Rather than examples of harmful data-enabled market power that allows them to stifle competition in downstream markets, the IoT business models provided by telecom operators (often in cooperation with IoT OEMs based on commercial contracts) are examples of precisely the kind of value-added services the DA proposals are meant to encourage.

Consequently, telecom operators are not the intended subject of a new B2B/B2C data-sharing obligation as envisaged in the EC's Impact Assessment. This is clear from the problem descriptions provided in the Impact Assessment, where a "mobility service provider" is used as the example of a data holder abusing their ability to foreclose access to their mobility data to force unfair contract terms on a start-up wishing to use this data for a value-added service[38]; while "location data coming from mobile network operators" is used on the next page as an example of "essential" data in a B2G context (public authorities' response to COVID-19).

Fundamentally, data held by telecom operators needs to be distinguished from the type of OEM data that are targeted by the Data Act proposal for the simple reason that telecom operators do not have unique access to specific data types in the way that OEMs have access to data produced by their connected devices.

For data-enabled downstream services, which are competitive (there are multiple sources of the same or equivalent data, which is incidentally illustrated by the Impact Assessment, which lists mobility service providers and mobile networks as sources of useful mobility data), there is no rationale for special data sharing rights outside normal commercial negotiations.

In fact, the only data held by telecom operators (other than in cases where they are OEMs or have otherwise control over data originating from connected devices) that are uniquely generated by them is ECS data. Here we note that ECS data and its use is heavily regulated, both limit its usefulness in the context envisaged by the EC and would impose unique burdens on telecom operators (some of the ECS data potentially in scope would not be processed or stored at all if it were not for regulatory reasons).

In addition, IoT connectivity is an inherently global business, with IoT objects often moving across different networks. This is possible due to roaming agreements between telecom operators, but that means that in practice a given network operator only ever has insights in their own network data – not those of other network operators.

[36] European Commission (2022) Commission Staff Working Document – Impact Assessment Report. Page 7. Available at https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act

[37] Ibid.

[38] European Commission (2022) Commission Staff Working Document – Impact Assessment Report. Page 11. Available at https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act

At the same time, telecom operators might be first in line for burdensome data sharing requests for economic reasons: telecom operators have ongoing customer relationships (contracts, billing etc.) with users and are based on the same jurisdiction, whereas OEMs often do not and are not, making the telecom operator the cheaper addressee of data sharing requests. This is especially problematic in the case where a third party wants to use the access right to assemble a larger dataset including the data from many different users, where targeting the request at the telecom operator may be much more efficient than targeting several different OEMs (e.g., the 'mobility service providers mentioned in the Impact Assessment but scaled across different cities).

This adds weight to the argument that data access rights should be enforceable against OEMs, rather than telecom operators, who don't have market power in relation to data generated by connected devices, and that in cases where the telecom operator is the appropriate addressee of an access request, it should be fairly compensated (irrespective of the source of the request).

**Recommendations**

The market for connected devices, related services, and the data they generate is still in an early stage of development. Any **regulation of these nascent markets should proceed with caution**.

The Data Act should support the competitive market by **ensuring fair compensation on commercial terms for any data sharing between firms** wherever possible. Accordingly, the Data Act should clarify responsibilities of different parts of the value chain (especially in relation to resellers of IoT devices) and recognise the full extent of the costs and liabilities involved.

Key concepts in the Data Act require clarification to ensure the Act is appropriately targeted. "IoT devices", "virtual assistants", "product", "service management layer", and "related services" need to be clarified and explicitly **state what products/services are included and excluded.**

Data generated by the operation of an electronic communications service ("ECS data"), including traffic data, location data and communication. **ECS data should be explicitly excluded from the scope of the Data Act,** as the existing regulation of collection and use of this data (notably the ePrivacy Directive) put it in a distinct category and must therefore be clearly distinguished from device data that has been generated using an IoT product or product related service.

The Data Act proposal should therefore be harmonised and coordinated with the ePrivacy rules, to ensure there is no legal conflict between the Data Act and sector-specific rules pertaining to communications data, where confidentiality of communications considerations apply.

There is no rationale for different levels of protection for "products" (Art 4(4)) and "related services" as the same rationale "to avoid undermining the investment incentives for the type of product from which the data are obtained" (Recital (28)) applies to related services.

## 6.2 B2G data sharing provisions

That data held by private sector organisations can play an important role in the fulfilment of important tasks for the benefit of the public has been amply demonstrated, notably in the context of the COVID-19 pandemic, but also in many other contexts where data such as mobility data collected by telecommunication networks has enabled greater efficiency in the public sector, from long term planning to real-time emergency response.

However, the provisions in the Data Act that deal with B2G data sharing are overly broad and risk excessive demands for data sharing from public sector bodies. This is especially problematic as the

Act fails to guarantee adequate compensation for data holders required to share data. The Act should be refined to focus on strengthening and building upon existing data sharing initiatives that have proved their usefulness, while treading carefully when it comes to speculative uses of data for which infrastructure and absorptive capacity on the part of the public sector bodies' may not exist.

**Recommendations:**

**The definition of concepts such as "public emergency" and "exceptional need for data" need to be clarified and circumscribed.**

Access obligations, as a measure of last resort, should be limited to clearly specified cases of truly exceptional nature (e.g., officially declared public emergencies) and include safeguards that any data provided cannot be used for purposes other than the one for which it is requested.

The Data Act should **recognise that adequate compensation (cost recovery at a minimum) is required** to incentivise ongoing investment in data infrastructures.

## 6.3 Data processing service switching obligations

A competitive market for data processing services is a precondition for a thriving digital economy. Market features such as onerous and lengthy switching processes and high egress fees deserve close scrutiny, and conduct requirements targeted at powerful market players such as hyperscale cloud service providers may be an effective tool in this regard.

At the same time, it should be recognised that the market for data processing services is diverse and includes many multi-party business models for which a simple division into powerful sellers and weak customers is inaccurate.

In addition, regulation should be sensitive to the real technical constraints that complex, high volume data processing services operate under, including in relation to switching. Rigid rules that assume that one size fits all are unlikely to meet the Data Acts pro-competitive objectives.

**Recommendations**

The Data Act should **clarify who is responsible for the switching process in multi-party business models** and ensure that resellers, who are simply reselling a cloud service offered by a third-party, have a legal claim vis-à-vis said third-party to ensure the effective implementation of switching requirements for their customers.

The Act should be modified so that cloud service providers and their enterprise customers can **agree on a different notice and switching period,** in particular if this benefits the customer.

# Index of Tables, Figures and Boxes

## Tables



## Figures

## Boxes

# Annex 1 Stakeholder consultation Guide

Stakeholder consultations were carried out with various ETNO members. These interviews contributed to our understanding of the potential impacts of the Data Act on the various business models that Telecom companies operate.

**Table 5 Stakeholder interviews**

| Date | Company | Names of interviewee(s) |
|---|---|---|
| 13/06/2022 | Vodafone | Matthew Allison |
| 22/06/2022 | Telia | Tatjana Lukoševičienė, Charlotte Lundell Berg, Kristofer Agren |
| 23/06/2022 | TIM | Claudia Gerbino, |
| 27/06/2022 | Deutsche Telekom | Valentin Steinhauer |
| 29/06/2022 | Telenor | Krisztina Baracsi |
| 02/08/2022 | Telefonica | Cristina Vela Marimon |
| 06/09/2022 | Orange | Coline Dimbour, Sara Bussiere & colleagues |

## A1.1 Introduction

In ETNO's initial assessment the proposed Data Act ("DA") affects the business models of telecommunication network operators in general in the following three scenarios:

1) B2C and B2B data sharing – As providers of connectivity in IoT environments, where the role of telecommunication network operators in data processing is set to evolve with 5G (e.g., smart homes, connected cars, industry 4.0). Additionally, as providers of related services or virtual assistants, e.g., when providing data sharing platforms or applications/platforms that enable control or access to connected devices (e.g., in Smart Home context).
2) B2G data sharing – As providers of network data (e.g., traffic and location data) to public authorities, also considering their existing big data analytics offerings for public sector customers.
3) Data processing services switching, interoperability, and data access – As providers of cloud and edge services (especially to business customers) and as customers and system integrators in Multi-Access Edge Computing (MEC) and network virtualization solutions (e.g., Open RAN). Risks and opportunities should also be assessed in light of telecom operators' strategic partnerships with hyperscale cloud providers

## A1.2 Business models and products affected by the DA

Which telecom services and offers are affected, including the specific data categories that are in the scope of the DA (and specifically in the scope of the sub-chapters on business-to-consumer, business-to-business, and data processing services)?

- Products may include: ISP modem; Private & public 5G/LTE networks, sub-components in IoT devices (e.g. SIM in connected car).
- Related services may include: aftermarket repair and maintenance services and access to diagnostics information; private & public 5G/LTE networks; IoT related applications and platforms (e.g., application to control Smart Home devices);
- Virtual assistants may include IoT related platforms and applications; voice assistants; etc.

Are any of these services and products not covered by the DA in your view? Are there any others that could be impacted?

Can you provide concrete examples, especially regarding forward-looking 5G services?

## A1.3 Scope of the DA

What are the areas in which the scope of the DA is unclear or ambiguous? (E.g., definition of data, delineation between 'genuine IoT data generated by connected objects' and 'communications related data' generated by end user devices, hardware, software, intelligent networks, etc. (what about data generated by (parts of) an electronic communications service network such as those for mobility solutions? What about aggregated traffic & location data or similar data from electronic communications services?)

What is the most adverse/benign interpretation? Could the current wording of the proposal be clarified to create more legal certainty for telecom operators (e.g., clearly state that ECS are out of scope of related services)?

## A1.4 Interplay with the existing EU regulatory framework

Where do you see the DA interacting with regulation on data already applying to the telecom sector (GDPR, ePrivacy, others)? What frictions do you foresee?

## A1.5 Impacts of the DA

What do you see as the key impacts of the DA?

Does the DA's focus on content and apps providers increase the risk for telecom operators as connectivity providers?

With specific reference to data processing services, what impacts do you expect as a result of easier switching, portability, and greater interoperability on telecoms' cloud and edge computing key offerings to business customers, as well as on their relationship with cloud infrastructure and edge providers (e.g., hyperscalers) as customers/strategic partners?

Which IoT related use cases from the telecommunications sector are in the biggest danger of 'free' data access in the B2B, business-to-(end-)user (B2U) or B2G scenarios?

How do the B2B data sharing rules affect how connected products are delivered (directly or in collaboration with 3rd parties)?

What impact do you see on 5G network slices and 5G services?

Have you done any modelling of these impacts? Is there any quantitative analysis you are aware of?

## A1.6 Opportunities for telecom operators

What do you see as the key business opportunities enabled by the DA (for your business and the telecom operator sector more broadly)?

## A1.7 Key areas of concern & possible improvements of the DA

What do you see as the key improvements that could be made to the DA to reduce the risk to your business models and increase the opportunities it presents?

# Annex 2 Survey on business models

The survey was distributed to ETNO members to gain an understanding of how ETNO members perceive the risks and opportunities of the Data Act.

## A2.1 B2B/B2C Data sharing

**Table 6 Scenario 1A – both hardware and services/management layer supplied by telecom operator**

| | |
|---|---|
| Do you operate this business model? | Yes / no |
| Please provide examples. | **….** |
| How important is this business model for your business overall? | (Very important) 1…2…3…4…5 (Not at all important) |
| Do you currently provide data generated under this business model under commercial data sharing agreements? | Yes / no |
| What data does this involve? | ….. |
| How important is commercial data sharing for your business overall? | (Very important) 1…2…3…4…5 (Not at all important) |
| Would the proposed Data Act create additional costs for you? | A) operational costs (e.g. staff time for responding to sharing requests)<br><br>(Very high additional costs) 1…2…3…4…5 (no additional costs)<br><br>B) other costs (e.g. reengineering components to enable external data access) |

| | |
|---|---|
| | (Very high additional costs) 1…2…3…4…5 (no additional costs) |
| Would the proposed Data Act create business opportunities for you as a result of increased access to data held by other organisations? | (Very significant opportunities) 1…2…3…4…5 (no opportunities) |
| Describe potential opportunities | |

**Table 7 Scenario 1B – services/management layer provided by telecom operator, hardware supplied by 3rd party**

| | |
|---|---|
| Do you operate this business model? | Yes / no |
| Please provide examples. | **….** |
| How important is this business model for your business overall? | (Very important) 1…2…3…4…5 (Not at all important) |
| Do you currently provide data generated under this business model under commercial data sharing agreements? | Yes / no |
| What data does this involve? | ….. |
| How important is commercial data | (Very important) 1…2…3…4…5 (Not at all important) |

| | |
|---|---|
| sharing for your business overall? | |
| Would the proposed Data Act create additional costs for you? | A) operational costs (e.g. staff time for responding to sharing requests)<br><br>(Very high additional costs) 1…2…3…4…5 (no additional costs)<br><br>B) other costs (e.g. reengineering components to enable external data access)<br><br>(Very high additional costs) 1…2…3…4…5 (no additional costs) |
| Would the proposed Data Act create business opportunities for you as a result of increased access to data held by other organisations? | (Very significant opportunities) 1…2…3…4…5 (no opportunities) |
| Describe potential opportunities | |

**Table 8 Scenario 1C – services/management layer provided by 3rd party, hardware and connectivity supplied by telecom operator**

| | |
|---|---|
| Do you operate this business model? | Yes / no |
| Please provide examples. | …. |
| How important is this business model for your business overall? | (Very important) 1…2…3…4…5 (Not at all important) |
| Do you currently provide data | Yes / no |

| | |
|---|---|
| generated under this business model under commercial data sharing agreements? | |
| What data does this involve? | ….. |
| How important is commercial data sharing for your business overall? | (Very important) 1…2…3…4…5 (Not at all important) |
| Would the proposed Data Act create additional costs for you? | A) operational costs (e.g. staff time for responding to sharing requests)<br><br>(Very high additional costs) 1…2…3…4…5 (no additional costs)<br><br>B) other costs (e.g. reengineering components to enable external data access)<br><br>(Very high additional costs) 1…2…3…4…5 (no additional costs) |
| Would the proposed Data Act create business opportunities for you as a result of increased access to data held by other organisations? | (Very significant opportunities) 1…2…3…4…5 (no opportunities) |
| Describe potential opportunities | |

## A2.2 B2G data sharing

**Table 9 Business to government data sharing**

| | |
|---|---|
| Do you currently provide data to public | Yes / no |

| | |
|---|---|
| sector organisations under specific contracts? | |
| Please provide examples | 1) …..<br>a) In this example, the data is provided a) on standard commercial terms b) at cost c) pro bono / free of charge d) other (please explain)<br>2) …..<br>a) In this example, the data is provided a) on standard commercial terms b) at cost c) pro bono / free of charge d) other (please explain)<br>3) …..<br>a) In this example, the data is provided a) on standard commercial terms b) at cost c) pro bono / free of charge d) other (please explain)<br>….. |

## A2.3 Data Processing Service Switching

**Table 10 Scenario 3A: Telecom operators as cloud suppliers using their own infrastructure**

| | |
|---|---|
| Do you operate this business model? | Yes / no |
| Please provide examples. | **….** |
| How important is this business model for your business overall? | (Very important) 1…2…3…4…5 (Not at all important) |

**Table 11 Scenario 3B: Telecom operators as resellers of 3rd party cloud services**

| | |
|---|---|
| Do you operate this business model? | Yes / no |

| | |
|---|---|
| Please provide examples. | …. |
| How important is this business model for your business overall? | (Very important) 1…2…3…4…5 (Not at all important) |

### Table 12 Scenario 3C: Telecom operators as Managed Service Providers (MSPs) of 3rd party cloud services

| | |
|---|---|
| Do you operate this business model? | Yes / no |
| Please provide examples. | …. |
| How important is this business model for your business overall? | (Very important) 1…2…3…4…5 (Not at all important) |

### Table 13 Scenario 3D: Telecom operators as consumers of cloud services

| | |
|---|---|
| Do you operate this business model? | Yes / no |
| Please provide examples. | …. |
| How important is this business model for your business overall? | (Very important) 1…2…3…4…5 (Not at all important) |

LE Europe

35 rue du Congrès,
1000 Bruxelles, Belgique
info@londoneconomics.co.uk
www.le-europe.eu
@le_europe
+32 2 229 19 02