Joint ETNO and GSMA position on the EC proposal for a Data Act

July 2022

1. Introduction

ETNO and the GSMA, who represent the telecoms sector in Europe and worldwide, welcome the Data Act proposal of the European Commission.

We support the objective of fostering data sharing and re-use across sectors and national borders in the single market that underlies the proposed Data Act. However, as the European Commission states in the proposal, that should not be detrimental to innovation, competition and incentives to invest in ways of generating value through data.

ETNO and the GSMA would like to suggest some improvements that are necessary for the regulation to meet its objectives and bring real value with benefits for EU citizens, companies and public administrations.

Please find below a **summary of the main issues** we would like to raise in the context of this consultation:

B2C and B2B data sharing

- Concepts such as 'product' and 'related services' need to be more precisely defined. IT devices like smartphones and personal computers should clearly fall outside the definition of 'product'. The definition of 'related services' should be addressed to services that are directly related to the product offering and the functionalities of the product itself, whereas electronic communication services (ECS) and the data generated by them should be excluded as they are used in the management and operation of the underlying connectivity.
- The proposed Regulation should distinguish between users' own data, and additional proprietary data insights that the data holder may invest in generating and, therefore, be entitled to a fair and reasonable remuneration for such data.
- The provisions on the sharing of data along the value chain of the IoT may need to be adapted to consider the specificities of different sectors and the need to protect Intellectual Property Rights such as trade secrets. A clarification of the practicalities of implementing data sharing, most notably regarding the need to protect personal data, is also needed.

Data processing services

- We support the propositions regarding switching and interoperability, but caution that the implementation of these provisions should be technically feasible.
- A contractual requirement imposing a maximum notice period of 30 calendar days for terminating a contract could be challenging for more complex or customized cloud projects. Contracting parties should be able to choose a longer notice period.

- The Data Act should be more precise regarding the charges in scope to avoid unintended effects on third party service providers.
- The obligations of the different actors involved in the data processing service value chain should be clarified, considering the different business models for the provision of the service (i.e. managed services, pure resale, or cloud broker) so that the responsibility along the value chain be correctly allocated. The party that has the contractual relationship with the customer and the provider of the technology in use do not always correspond. Switching should be the responsibility of the party that operates the underlying technology.

B2G data sharing

- It is necessary for the driving principles of B2G data sharing outlined in the Data Act to set the right incentives for a sustainable cooperation, including through fair and reasonable compensation for data supplied to public bodies.
- Voluntary cooperation should continue to be the default route for governments to obtain data from private companies, and therefore the Data Act must be more precise when it comes to the definition of the exception from this rule. The text should more clearly delineate the types of situations that would constitute a 'public emergency'.
- Only where there is a clear market failure that justifies regulatory intervention, mandated B2G data access should be considered as a measure of last resort and for a strictly circumscribed set of 'exceptional needs', to avoid crowding-out the innovative solutions available in the market.
- The requirement to provide data 'without undue delay' is very concerning, and should be adjusted to allow for an ambitious yet realistic timeframe that acknowledges both the public interest to be able to respond quickly to an emergency and the time needed for a private company to respond to the request.
- We welcome the Regulation's approach to account for compensation with 'reasonable margin' and we believe that a compensation of costs also during public emergencies would be appropriate.

2. A call for innovation conducive rules for B2C and B2B data sharing

The number of total active IoT connections is expected to reach **850 million in Europe by 2029**[1]. The telecom sector will be a key enabler of IoT ecosystems for people and businesses, from smart devices to industry 4.0. Very high speed connectivity and the maturing of the 5G networks will enable new streams of data coming from millions of connected sensors.

We welcome the Data Act's objective to facilitate data sharing for IoT devices and IoT-related services. Where possible, data exchanges should continue to be primarily based on voluntary agreements that address the specific needs of contractual parties, subject to general contract and competition law.

Actions that facilitate data access by users of connected products, and that increase transparency and fairness in data marketplaces, are welcome. Contractual parties that suffer from a weak negotiation position or face complex arrangements, such as in data co-creation models, stand to benefit from greater clarity on respective rights and obligations. We stress that fairness and non-discrimination provisions should remain strongly anchored in the principle of freedom of contract.

Key definitions need clarification

Legally binding rules on access to user-data from IoT devices can help to put users in control over who can use their data and under which conditions, while opening the aftermarket for third-parties and thereby increasing competition and user choice. While we welcome these objectives, we believe that several terms and concepts (e.g. 'product', 'related services', 'virtual assistants') in the proposal need to be more precisely defined and better targeted.

To increase legal certainty, legislators should better clarify **which devices would fall under the scope of a 'product' in Art. 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. These devices that 'include certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service' (such as for example smartphones or personal computers) are excluded from the definition of a 'product'. It should be further stressed, as to clarify that data generated in the management and operation of the underlying connectivity services (e.g. mobile location data[2]) are out of scope of these measures.

Therefore, ETNO and the GSMA argue for **the necessity to amend this definition to clearly exclude products mentioned in the recital 15**, which is also advised by the EPDB and EPDS in their opinion on the Data Act. More clarity would help to avoid conflicts of laws affecting digital products and services, especially with privacy and data protection rules that impinge on the usability of personal information generated by digital products[3].

[1] State of Digital Communications, 2022.
[2] Such as Call Detail Records (CDRs) and eXternal Data Representation (XDRs).
[3] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

Certain services such as companion apps (e.g. a fitness tracker that comes with a dedicated app) can form and integral part of the product experience and functionality of an IoT device and are therefore covered under the term 'related services' by the Data Act. However, such **'related services' need to be clearly distinguished from electronic communication services (ECS)**. ECS provide the connectivity necessary for many smart devices to function and communicate with other devices and services, however an ECS is typically not related to a *specific functionality* or product as such but is the medium through which data are transmitted. Therefore **the definition of 'products' and 'related services' should be clarified to exclude ECS and connectivity data from the scope of the data sharing obligations**. Without such a clarification, the regulation would risk creating onerous and disproportionate regulatory obligations for telecommunications service providers and actually run counter to the original intention of the proposal.

In fact, **we believe that the definition of related services should be more clearly addressed to services that are directly related to the product offering**, e.g. as part of the sales, rent or lease agreement. Recital 16 specifies that the definition of *related services* in Art. 2 (3) should also apply to services that are '*normally provided for products of the same type and the user could reasonably expect them to be provided*'. This wording is too vague and would risk including services that are provided by third parties which are entirely independent from the original product.

Data access requirements need a careful balance of interests

The Data Act aims to strike a balance between improved data access and the need to continue incentivising investments in data generation. Against this backdrop, the proposal states that a **third party data recipient** is prohibited to use the data obtained under the Data Act for the development of a product that would stand in direct competition with the device the data originated from. However, this protection for IoT products is not extended to related services or virtual assistants despite the fact that the data can also be obtained from these sources.

This means that a provider of a related service (e.g. a smart home app) could be required to provide data to a third-party based on a user request. This third party could then use the obtained data to develop a directly competing service. In contrast, such a situation would be prohibited when the data is obtained from a 'product' (e.g. a vehicle). Thus, it remains unclear why providers of 'related services' or 'virtual assistants' should not benefit from the same protections as the manufacturers of IoT products, given that they are subject to the same set of data sharing obligations.

At the same time, ETNO and GSMA appreciate that undertakings designed as **gatekeepers** under the Digital Markets Act are not an eligible recipient of the data generated during the use of IoT products, as to avoid further strengthening the position of already dominant players in the market. This carve-out is consistent with the findings of the European Commission's competition sector inquiry into the consumer IoT.

Moreover, the current DA proposal establishes that **'users'**, defined in the DA as individuals and companies, will access cogenerated data free of charge with the possibility to give access to such data to the third parties of their choice. ETNO and the GSMA think that it is important the proposal

distinguish the users' own data that they have contributed to generate, and additional proprietary data insights that the data holder may invest in generating and, therefore, be entitled to a fair and reasonable remuneration for such data. Fairness and non-discrimination provisions should always apply and data used for commercial purposes should be always subject to fair remuneration.

Finally, ETNO and the GSMA agree with the French Presidency progress report[4] noting that the provisions on the sharing of value along the value chain of the IoT may need to be adapted to take into account the specificities of different sectors and the need to protect Intellectual Property Rights such as trade secrets. We would also argue for a clarification of the practicalities of implementing data sharing, most notably regarding the need to protect personal data.

3. Opening up possibilities in the cloud and edge market

Edge cloud computing and cloud-based infrastructure are areas where Europe has the opportunity to invest and scale up capacity, establishing a degree of strategic autonomy that has not existed in traditional, centralised cloud markets, largely dominated by non-European hyperscalers.

The dependency on very few cloud giants that dominate the global cloud market has raised concerns about vendor lock-in, bargaining power, privacy, and transparency. The Data Act's propositions regarding switching and interoperability, create opportunities for a more competitive cloud and edge market in Europe, where more cloud services are offered in line with EU values and increased competition between service providers helps to drive down costs for consumers and increase opportunities for them to maximize the value of their own data.

As more and more consumers, governments and companies depend on cloud services, it becomes all the more **vital to create a more open and dynamic cloud market**. By enhancing the 'switchability' of cloud services, the Data Act can contribute to increase flexibility and choice for customers while reducing dependencies resulting from vendor lock-in.

However, it is also important to consider that the cloud market is evolving and in parallel to providing standardized off-the shelf solutions it also addresses more specialized needs as it is the case of Multi-access Edge Computing (MEC) for ultra-low latency and high bandwidth radio telecommunications network.

Switching and portability processes should be proportionate to the technical complexity

While welcoming the general objectives on cloud switching, ETNO and the GSMA would like to stress that the implementation of provisions on the Data processing services chapter should be **technically feasible** and should not hinder innovation and business opportunities in the cloud and edge cloud sectors, which are strategic sectors for the digitalization of the economy and society.

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

Removing obstacles for better switching between data processing services is welcome. However, the obligation to include a contractual requirement imposing a maximum notice period of 30 calendar days for terminating a contract could be challenging for more complex or customized cloud projects, e.g. requiring 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. ETNO and GSMA support the inclusion of a provision leaving the choice for contracting parties to negotiate and allow for a longer notice period.

While we generally welcome that Art. 25 limits the charges that can be imposed by the data processing provider on the customer, within the limits for the data holder in providing communication interfaces (API where possible), the Data Act should be **more precise with regard to the charges in scope** to avoid unintended effects on third party service providers. While it must be ensured that data processing providers cannot impose fees for data export that would effectively hinder or discourage a customer from switching, this does not necessarily mean that switching automatically comes at no price.

In practice, some cloud customers might rely, for example, on external service providers for the implementation of complex cloud migration projects. If the switching process would have to be always free of charge, such external service providers would no longer be able to charge for the time and effort it takes to assess the feasibility of an alternative platform and to plan, test and execute the re-architecting and migrating of applications or entire application landscapes to an alternative ecosystem.

This would run counter to the original intention of the Data Act to create an open market for cloud services in which service providers can compete and offer their solutions to customers who often depend on the provisioning of such **specialized services**, including for complex switching or migration projects. Legislators should therefore clarify that the abolition of "switching charges" does not preclude the possibility of a third-party provider to be compensated for specialized services offered to support the switching process.

Responsibility for switching and portability should be fairly allocated

First, ETNO and GSMA suggest to clarify that **data generated by ECS is not subject to the cloud switching process** in respect to the portability obligation.

Second, ETNO and GSMA would like to point out that the proposal may benefit from some clarification as to the obligations of the different actors involved in the data processing service value chain, taking into account the different business models for the provision of data processing services (i.e. managed services, pure resale or cloud broker), in order to **correctly allocate the responsibilities along the value chain**, considering that the party which has the contractual relationship with the customer is not always the provider of the technology in use.

The current proposal focuses mainly on contractual obligations. This raises the question as to who is legally obliged to implement the requirements of the Data Act in situations where the contracting party is not the same as the original technology provider. It is important to note, that resellers often offer a complete product whose essential features are determined by the technology provider. An important part of the switching process however relates for example to the technical adaptation of a customers' data, applications and digital assets. This cannot be achieved by a reseller but must be implemented by the technology provider.

Therefore, the Data Act should be clear that **switching is the responsibility of the party that operates the technology used**. Resellers, managed service providers, cloud broker lack control over the product management and operations of the underlying technology. Hence, the Data Act should not lead to situation where resellers, managed service providers or cloud broker are legally obliged to guarantee switching while being dependent on the technology provider for the actual implementation. Hence, where the technology provider is not the same as the contracting provider (e.g. reseller, managed service provider, cloud broker), it must be ensured that the latter has a **legal claim towards the technology provider** for the effective implementation of requirements.

4. Need for sustainable B2G data sharing cooperation

Telecommunications operators have a long history of cooperation with public administrations, typically by providing insights based on aggregated and anonymised network data to tackle epidemics and other societal challenges. Collaboration will undoubtedly continue in the context of our sector's social commitment. Separately, it is important to think of cooperation also in terms of opportunities and ways to strengthen Europe's data economy.

However, for B2G data sharing to be successful, it is necessary to **set the right incentives for a sustainable cooperation**, including through fair and reasonable compensation for data supplied to public bodies.

The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) stressed in their opinion on the Data Act that they 'have serious concerns on the lawfulness, necessity and proportionality of the obligation to make data available to public sector bodies and Union institutions, agencies or bodies' included in the Chapter V of the proposal[5]. Many important questions remain unaddressed, for example how the public sector can build-up the capacities and structures needed to make use of the data obtained while handling sensitive customer data in a responsible way.

ETNO and the GSMA think that the **driving principles of B2G data sharing** should be:

[5] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

- **Voluntary cooperation** between businesses and governments should continue to be the default route for B2G data sharing. Legislators should specify more clearly when an 'exceptional need' would justify the introduction of an access obligation.
- the **notion of public emergency must be clearly and narrowly defined in the regulation, in particular in light of the possibility for a public sector body to request data preemptively, i.e. prior to the emergency taking place (Art. 15(1b)); and should not be extended** to a point that hinders the development of data analytics solutions;
- Legislators should clarify why and under which conditions an access obligation would be required for cases other than emergencies, starting by defining the types of activities that would qualify as 'tasks in the public interest' (Art. 15(1c)).
- companies' **costs for providing data should be compensated also during emergencies**, including the costs of anonymization and pseudonymization processes;
- public authorities should **choose the best quality and the most cost-effective data provider** for emergency data set; for example, by requiring mobility data from GPS-based players;
- in case public authorities should require **data analytics from data holders,** third parties should only be involved with the explicit permission of the business having shared the data initially;
- The proposed timescales for compliance with a data request (**'without undue delay'**) need to be adjusted to reflect commercial, operational, and technical limitations. This relates in particular to cases where personal data are requested requiring the application of adequate safeguards (e.g. pseudonymization) prior to the data transfer.
- **liabilities** regarding individual data protection rights, trade secrets and intellectual property **should rely on public authorities**.

We will elaborate more on the abovementioned issues in the following sections below.

Timescale for compliance

The requirement to **provide data 'without undue delay'** in article 18.1 is very concerning.

The ability of private companies to provide data to the public sector is limited due to technical, organizational, and legal constraints. First, the volume and nature of data that can be delivered is limited due to storage capacities, the data format used, and compliance with legal requirements. Second, some data might not be collected at all or is only available at pre-defined time intervals. Hence, it is important to take these constraints into account.

Furthermore, it is important to acknowledge the time needed for a private company to:

1) verify (and potentially challenge) the request;
2) agree on the data to be provided in light of the exceptional need and check the availability and nature of the data requested;

3) ensure that all necessary technical measures are taken to protect customer data (e.g. pseudonymization/anonymisation);
4) and to make the organizational and technical resources available to process the data and provide it to a public sector body.

While we understand the need to obtain data quickly in times of crisis, the current timescales included in the proposal appear unrealistic from a practical perspective. They need to be adjusted to allow for an ambitious yet realistic timeframe that takes into account both the public interest to be able to respond quickly to an emergency and the time needed for a private company to respond to the request.

Additionally, we would like to emphasize that authorities need to invest into emergency preparedness, which also includes collaboration with private actors before an emergency, e.g. in the form of research collaboration, so that response can be sped up in case of an emergency.

Public emergencies definition (Article 2)

We strongly believe that **voluntary cooperation** should continue to be the default route for governments to obtain data from private companies. The Data Act therefore needs to be more precise when it comes to the definition of the exception from this rule. While the intention to restrict data access obligations to cases of 'exceptional need' goes into the right direction, the current proposal leaves too much room for interpretation.

In this context, ETNO and the GSMA recommend to **refine and tighten the definition of public emergencies** in Article 2(10), which is currently too broad and does not provide enough legal certainty. Therefore, we support the suggestion of the EDPB and EDPS to amend the definition and more clearly delineate the types of situations that would constitute a public emergency.

Additionally, we would recommend to better qualify the notion of '**major cybersecurity incidents**' as an example of public emergencies (recital 57) as this is not defined in the text and does not qualify as a public emergency *per se*. For better clarity, we recommend to delete or, at a minimum, amend the reference to **make it clear that a cybersecurity incident does not constitute an emergency in itself but could – under clearly defined circumstances – be a trigger** to a public emergency as defined in Art. 2(10).

Furthermore, we recommend referring to the concept of 'significant incident' as defined in the new NIS 2 Directive, which provides guidance on the identification of a cyber-incident as substantial based on its impact on critical services and people. Furthermore, reporting obligations in the event of cybersecurity incidents and data breaches are well-established in EU and national law. Public authorities already benefit from substantial information streams that allow them to analyse and cope with major cyber incidents. It should be clarified that the data requests issued by public authorities should not duplicate and overlap with the data collection carried out through the existing incident notification mechanisms.

Exceptional needs to use data circumstances (Article 15)

We acknowledge the public authorities' need to make sure they have access to the data required to respond to exceptional circumstances. The analytical solutions that already today are offered by some telecom operators and other players can inform authorities' decision-making in certain public policy fields based on previous experience (e.g. pandemics), with benefits in terms of cost efficiency and quality of the insights.

Only where there is a clear market failure that justifies regulatory intervention, mandated B2G data access should be considered as a **measure of last resort and for a strictly circumscribed set of exceptional needs**, to avoid crowding-out the innovative solutions available in the market.

As mentioned by the European Commission Regulatory Scrutiny Board and in the French Presidency Progress Report[6], we support the idea that 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 to public sector bodies large room for interpretation, especially the point (c).

The current reference to fulfillment of **'tasks in the public interest'** could cover anything from mobility management to urban planning or the compilation of official statistics. If such a category is indeed included in the final text, the term 'public interest' needs to be much clearer defined, including by specifying the types of situations in which an access obligation would be justified. The requirement that such activities need to be provided for by law seems overly broad given that most, if not all, activities of the public sector would fall under this category. As is stated, we support the EDPB and EDPS opinion finding the provision problematic, raising also fundamental rights interference issues[7].

We welcome that the Commission has built in a **market failure test** in Art. 15 (c1) that requires the public sector body to exhaust all available alternatives to obtain data from the private sector before making use of an access obligation, e.g. via normal contractual negotiations. This is a crucial element to avoid undermining / crowding out existing private sector initiatives. However, such a market failure test should be based on verifiable criteria and clear safeguards for the data holder, to avoid this provision leading to a weakened negotiating power of the data holder when negotiating the economic conditions for providing data.

Recital 58 states that the public sector body should demonstrate '*that no alternative means for obtaining the data requested exists*'. However, it remains unclear who will assess whether such possibility in fact existed and on what basis. Moreover, the proposal in Art. 15 (c) point 2 foresees a derogation from the market failure test in case this would reduce the administrative burden for the data holder or "*other enterprises*", leaving it unclear which other enterprises the proposal refers to. Legislators should close this existing loophole by clarifying that the only alternative to going to the market would be a request by the data holder itself.

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

[7] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

Compensation in case of public emergency and in case of exceptional need (article 20)

Public-private collaboration – which is generally based on voluntary contractual agreements – should ensure **fair compensation on investments made and costs incurred**. For this cooperation to flourish, it is crucial that data sharing agreements are based on reasonable terms in order to offer long-term sustainable solutions, including the possibility for operators to achieve a fair return on investments made in collecting and generating data. We also think, based on the COVID experience, that it is close to impossible to set apart data provision for the purpose of 'responding' to a pandemic as opposed to 'prevention' or 'recovery'. We therefore recommend that the Data Act is amended to ensure a clearer identification of the tasks of public authorities that are dedicated towards prevention and recovery (which should be subject to fair remuneration), and those that are related to immediate emergency response.

We welcome the Commission's approach to account for **compensation with 'reasonable margin'** for data being requested in situations other than in response to a public emergency. The Data Act proposal does, however, miss the opportunity to leave the option for a company to **determine whether there is a need for compensation also during public emergencies**. Given the significant uncertainty regarding the frequency and length of public emergencies that could fall under the obligations in Chapter V, we believe that a compensation of costs would be appropriate. This would still leave the possibility for companies to provide data for free, but it would prevent situations in which companies cannot recover any costs, even though they might be faced with an unexpectedly high number or long duration of data requests, and having to assist the interpretation of the data by public authorities.

Policy contacts:

Xhoana Shehu
Policy Officer, ETNO
shehu@etno.eu

Elizabeth Wiltshire
Manager, EU Affairs, GSMA
ewiltshire@gsma.com