European Telecommunications Network Operators' Association

ETNO policy position on the European strategy for data

Executive Summary

This paper outlines ETNO's views on the **European Data Strategy**, released by the Commission on 19 February 2020. The document focuses on the Strategy's approach to **data access and sharing in the business-to-business (B2B) and business-to-government (B2G)** contexts, also including B2B competition issues linked to exclusive data access. Furthermore, we elaborate on investment in data infrastructures, with emphasis on a **European cloud ecosystem**.

As big data will blossom at the intersection of 5G, the Internet of Things and Artificial Intelligence, the European telecom industry **applauds the Strategy's vision** for creating common European data spaces. We recommend that the Commission consider some key elements that, in ETNO's view, will be crucial to a successful single data market that drives innovation and competitiveness:

- **B2B data sharing** should generally continue to be based on **voluntary contractual agreements**, which address the conditions and specificities needed to make B2B sharing mutually beneficial in a flexible way. Barriers and uncertainties around data co-creation, sharing and use could be addressed by greater standardisation of contracts and datasets, use of data marketplaces, and support to data sharing and pooling partnerships.
- Solutions that **facilitate voluntary B2G data sharing**, such as contract and data standardisation and regulatory sandboxes, should be supported. **Mutually beneficial cooperation** between private and public sector requires legal certainty for data sharing in the public interest, fair compensation, and skilled public authorities.
- A two-pronged approach to preserve fair data access in digital markets and avert abuse of market powers by digital gatekeepers is needed. A **review of competition policy** to increase its effectiveness in the fast-changing digital markets should be complemented with an **ex-ante regulatory regime** that prevents competitive issues in a forward-looking manner. **Mandatory data access** for large online gatekeepers could be considered as a remedy.
- A **pan-EU interconnected "cloud federation"** could become the underlying infrastructure of the European data spaces and could reduce Europe's existing dependencies in this area. This would help achieve long-term data sovereignty goals. Synergy among the different funding programmes is key to the success of the project.

Background

World-class connectivity in 5G and fibre will be a key enabler of Europe's digital economy and of the increasing digitisation of services and industrial processes. **5G will enable the rapid growth of the Internet of Things (IoT)**: the number of mobile IoT connections in Europe is set to grow from 140 million in 2018 to nearly 740 million by 2026[1].

The massive amount of data generated by IoT connections and devices will create fresh resources for growing data analytics and **Artificial Intelligence (AI)** in Europe, which will give another boost to the competitiveness of the EU economy. As reckoned by the European Commission, by 2025 data analytics will take place mostly in connected devices and edge computing, which is underpinned by smart, software-defined 5G networks.

5G will then drive IoT, and IoT will in turn fuel European AI. Together they can form a truly powerful virtuous circle that creates a new promise for globally competitive European industries.

The success of this virtuous circle rests on the availability of a **crucial asset: data**. If Europe is to scale and compete globally in AI, new sources of large streams of data coming from millions of sensors connected over 5G will need to be exploited. Boosting the data economy is a cornerstone of Europe's digital leadership ambitions.

It is against this background that ETNO welcomes the **European Commission's communication on "A European Strategy for data"**, which sets the right vision and goals for creating a European single data market that drives competitiveness and builds a robust governance model – a 'European way' – in the global data economy.

We commend the Commission's commitments to achieving this bold vision by leveraging regulation, technical enablers, and competences to remove existing barriers to data sharing, pooling and scaling in a coordinated way, including the build-up of a European Cloud ecosystem.

Access to and usability of data are becoming determining factors for competition, innovation and value-creation – for private and public organisations alike.

Against this background, the key issue is how we ignite European growth and innovation through more and easier **data sharing between businesses (B2B) and with the public sector (B2G)**.

The following policy position thus focuses on the cross-sectorial measures for data access and use anticipated by the Strategy. We propose ways forward for an enabling framework regarding data access in B2B and B2G environments, particularly in the context of a future 'Data Act'.

We also outline some thoughts on how to effectively tackle **anticompetitive behaviour linked to data**, since businesses increasingly depend on data to remain competitive, with access to and usability of data becoming a determining factor for competition – or possible lack thereof.

Finally, we elaborate on the promotion of a **pan-European cloud ecosystem** that underpin the European data spaces and increase digital growth and sovereignty.

[1] ETNO, The State of Digital Communications 2020, January 2020.

Business to Business Data Sharing

Data-sharing is typically based on **contractual agreements** between the businesses concerned. These contracts usually define the conditions (duration, purpose, compensation) and restrictions for using data, thereby addressing the specific needs of the contractual parties. Voluntary data sharing is then governed by general contract and competition law.

When looking at cross-sector data sharing, there is no indication of systematic and structural market failure, namely of exclusive data collection and use as a crucial barrier to competition along the value chain. Horizontal, untargeted regulation obliging businesses to grant access to their data would then be unjustified. The introduction of cross-sectorial symmetric obligations would also not sufficiently reflect the specificities and characteristics of markets when it comes to data[2].

We thus consider that **B2B data sharing should generally continue to be based on voluntary contractual agreements**, as this presents a well-functioning and flexible way to sufficiently address the conditions and specificities needed to make B2B sharing mutually beneficial. We therefore agree with the Strategy's outline that "*the general principle shall be to facilitate voluntary data sharing*".

This does not exclude that access to data could be imposed in case of systematic market failure in a given sector, especially in situations where this would open-up secondary markets for complementary services.

Nonetheless, we agree with the Commission's assessment that **barriers to B2B data sharing** exist, due predominantly to lack of trust between business partners and insecurities around antitrust rules, privacy, trade secrets & intellectual property. This often goes together with the fear of sacrificing investment efforts or sharing competition-sensitive data. Furthermore, businesses often refrain from exchanging data more frequently due to regulatory restrictions for personal data and technical reasons, such as a lack of standardisation and interoperability of datasets.

In addition, while contract law provides stakeholders with a flexible toolbox to construct mutually beneficial arrangements, uncertainties remain when contractual parties find themselves in a weak negotiation position or face complex contractual arrangements such as in **data co-creation models**.

Consequently, we share the need to further improve voluntary sharing and re-use of non-personal data in B2B environments. To achieve this, we consider the following **key actions necessary** as part of the upcoming legislative framework for the governance of common European data spaces and the future Data Act:

- **Industry-led data marketplaces**[3] should be further promoted at EU level, as they are becoming a key driver for voluntary data-sharing. Common European data spaces will be created for multiple industries by enabling further research & development of various technological and

[2] The suitability of asymmetric ex ante access obligations, aimed at major players that leverage crucial assets such as exclusive access to data to entrench their dominance, is explored in a dedicated section below.

[3] For instance, Deutsche Telekom's Data Intelligence Hub (https://dih.telekom.net/en/) offers a market place for data and analytics, acting as a technical enabler and secure interface by which businesses can exchange data across sectors without losing "ownership" of the data. It builds on the open-source architecture of the International Data Spaces Association. The KPN Data Services Hub (more info here http://www.kpn.com/dsh) is a platform-as-a-service based on real-time information exchange. The platform is multi-tenant, so parties can work with existing data, without losing ownership off the data. The owner of the data retains control over competitive or business-sensitive information because all environments are separated from each other and remain under the owner's management.

conceptual data exchange components. ETNO members strongly believe that this can be achieved through the use of existing data exchange marketplaces as an initial testbed and proof of concept for more development in the area. These industry-specific marketplaces should be operated via a group of neutral, industry consortium members, to better ensure data sovereignty amongst members.

- The development of **contract model clauses** serving as a negotiation basis could help reducing uncertainties and guarantee equal partaking of the parties involved, e.g. in the context of co-generated industrial data. Interoperability is a critical factor for the data spaces to work. The development of **common standards/interoperability** for non-personal data should be intensified, by introducing an enabling European framework with technical solutions that help achieve data sovereignty, such as the IDSA architecture and the Gaia-X project. We also agree with the Strategy's aim to better harmonise the description of industrial datasets (metadata), in order to increase their usability and transparency for businesses (e.g. quality of data and storage information). We suggest that standardisation and interoperability of data formats could be tested on some key datasets from select sectors. A multi-stakeholder standard committee should be established to ensure feasibility and usability of the resulting interoperable data set.

The Commission should support these initiatives through dedicated funding under the Digital Europe, Horizon Europe, and Connecting Europe Facility programmes, which aim for the creation of European data spaces.

We also welcome the announced update of the Horizontal Cooperation Guidelines to facilitate **data pooling and data sharing agreements** among partners and competitors. Those initiatives help EU players to achieve competitiveness and to create innovative and interoperable products and services that support the broader EU competitiveness. Since these agreements need scale to become significant, ETNO supports a new block exemption for data sharing/data pooling agreements, as well as further guidance on this kind of agreements in the Guidelines.

Business to Government Data Sharing

Already today, some telecommunications operators collaborate with the public sector, typically by providing **mobile location data-driven analysis** to tackle epidemics, natural disasters, and environmental pollution. European telecom companies are helping public authorities react to the COVID-19 outbreak by giving them access to anonymous and aggregated location data to map out and predict the spread of the pandemic.

These examples are generally based on voluntary agreements, but oftentimes miss fair compensation on investments made (e.g. inherent costs of extracting, analysing and aggregating/safeguarding the data, including the frequency of sharing). For collaboration agreements to thrive in the future, it is therefore crucial that collaboration agreements are based on **mutually beneficial terms** that offer long-term sustainable solutions.

What keeps B2G collaborations from happening on a more continuous basis is thereby not the unwillingness to share data but rather operational barriers (e.g. high transaction costs) and technical

challenges (standardisation) that prevent them from scaling. This holds especially true for the public sector, which so far lacks the analytical ability and capacity to make enough use of the available data, including public data.

We therefore support solutions that **facilitate voluntary B2G data sharing**, such as:

- better **standardisation of contractual provisions** and **interoperability of data formats;**
- put the Commission's **2018 guidance on B2G data sharing**[4] , whose principles are redefined in the **B2G data sharing Expert Group Report**[5] up for testing, by launching a piloting phase that would allow businesses to give valuable feedback on established principles to assess their robustness in practice and consequently lead to market evidence as a basis for future considerations.
- create **regulatory sandboxes** and assess their effectiveness before taking additional, more prescriptive legislative measures.

Furthermore, the following conditions are a prerequisite to ensuring a mutually beneficial cooperation.

Public interest:

Any future framework should aim at clearly developing **criteria that define where there is "public interest"** in order to create legal certainty for the private sector. Public interest purposes for which data sharing can help may include, for instance, tackling high societal challenges like natural disasters and health epidemics such as the ongoing sharing of mobile data with several national health authorities to help limit the spread of COVID-19.

In circumstances other than tackling serious and immediate challenges like the above-mentioned emergency situations, combining data from different sources (e.g. location data and socio-economic profile data) with the public objective to produce insights for instance for city transport and mobility planners would risk crowding-out existing private businesses and initiatives.[6] The impact on innovation and competitiveness would be severe. Such purposes should consequently not fall under the notion of public interest warranting data access obligations. This incipient market should be expanded thanks to stimulating measures that allow it to reach its full potential.

Compensation*:*

Telecom operator's data such as location data are generally collected and processed as a by-product and come with considerable additional investments by operators.

For example, the provision of location data-based insights requires pre-processing, analysis and aggregation of such data, including anonymisation and secure transmission in compliance with strict data protection requirements set out both by the GDPR and the ePrivacy Directive. Making such data

[4] https://ec.europa.eu/digital-single-market/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy

[5] https://ec.europa.eu/digital-single-market/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more has redefined the principles of proportionality, purpose limitation, do no harm, transparency, accountability, fairs and ethical data use, conditions for data use and mitigate limitations of private sector data.

[6] For example, telecoms operators are already successfully working with public and private transport companies to help them improve their city infrastructure through the provision of mobile location data insights.

available to third parties (including time and resources for preparing and adapting them to the specific request and purpose) thus incurs significant costs.

Consequently, **fair compensation models** would need to be adequately addressed, balancing the need for investments on the data supplier side and the public interest of the public entity concerned. A fair compensation scheme will give businesses the necessary incentive to boost this market, whereas free data access undercuts any incentives to market development.

***Public Sector**:*

Today, the public sector is still far from being well-equipped to make use of and promote availability for its own public data. This holds even more true for privately-held data, linked to several reasons: public entities generally **lack digital skills for data analysis** and the necessary capacity to adequately deal with a variety of risks linked to data-sharing (e.g. potential disclosure of data sets revealing sensitive commercial information; responsible handling of aggregated data and applied safeguards like pseudonymisation, encryption).

To overcome these existing operational and technical gaps, it is thus necessary to **improve public sector capacities and digital skills** so that public entities can reap the full benefits of private sector data.

At the same time, public sector organisations largely rely on third parties to process and analyse the data received from private suppliers. These analytics solutions bring substantial benefits in terms of cost efficiency and quality of the insights. Therefore, the enhancement of public sector capabilities should not crowd-out the successful commercial solutions available. **Choice and variety of data analytics providers should be promoted**, to avoid that the bulk of outsourcing be seized by few data-dominant companies – with the risk of strengthening existing foreign tech giants even further.

Data and Competition: Access to Data as a Remedy

A large part of today's digital business models relies on data when designing and marketing services which go along with several benefits for users (e.g., increased convenience, personalisation, etc.). However, data might also be key to **market dominance and the abuse thereof**, helping companies to foreclose rivals, create and cement dominance on a durable basis, and leverage the accumulation of data to expand their dominance into neighboring markets. In such cases, exclusive access to data to the detriment of potential competitors can foreclose competition in a market.

Where a dominant company enjoys sole control over non-rivalrous data with competitive relevance and refuses to grant access to existing or potential competitors, foreclosure or even quasi-monopolisation are very likely to result. **Safeguarding fair data access** is thus key to ensuring healthy competition in those cases where data is not contestable.

Competition policy can tackle failures in digital market and recent European cases have demonstrated that the Commission can act strongly. Nevertheless, considering the challenges raised by the digital economy (speed, tipping markets, need for cooperation to innovate), an **extensive review of competition policy** is needed to make it more effective.

Mandating data access under EU competition law to remedy abusive behavior by a dominant firm could then be attained based on Article 102 TFEU: where data is regarded to be a key input, like in markets with strong direct and indirect network effects and economies of scale, imposed access could be the right tool to remedy abusive behavior based on exclusive control of data. These obligations would be necessary with regard to large platforms with strategic market status that, by controlling large amounts of data coupled with superior analytics capabilities and network effects, make their respective markets or even entire ecosystems in which they operate non-contestable for existing and potential rivals.

In practice however, mandating data access in case of abuse of dominance or as remedy imposed in M&A cases opens-up an array of unsolved questions and challenges, such as: setting detailed conditions for data access (which type of data, for which purpose and duration, potential compensation schemes), also considering the different market characteristics of the sectors concerned; the need to regularly update and adjust these conditions depending on changing market developments; and ensure continuous oversight on data access.

To address these questions and considering that very limited precedents exist so far, **further guidance and clarification** is needed under EU competition law on how to effectively impose data access obligations as a remedy for mergers and antitrust cases. Where justified in a given case, authorities should be encouraged to use data access obligations as an effective remedy.

Besides the need for an extensive review of competition policy in its application to the digital sector, we consider it is necessary to complement it with an ex-ante regulatory regime that tackle competitive issues more timely, on a prospective basis and thereby avoid durable and cemented dominance to manifest which would make markets or even entire ecosystems durably uncontestable. There are generally clear limits to what competition law can achieve, due to the lack of speed of current procedures, the backward-looking nature of antitrust cases, the case-by-case approach which is insufficient to tackle systematic and structural market failure, the dynamism characterising digital markets, and the limitation of enforcers with regards to necessary oversight of (real-time) data access and continuous monitoring of markets.

Since adaptations to competition law are insufficient to ensure effective competition on a forward-looking basis, before entrenched and durable dominance materialises, they should be complemented with a **targeted asymmetric ex-ante regulatory framework for systemic platforms** as a means to promote competition and the entry of new players. These rules may address, for instance, certain forms of interoperability or access to certain data that are essential to ensure competition.

Possible Modalities for Data Access

Since data access obligations should consider the different characteristics and specifications of the markets concerned (e.g. what types of data and usage are relevant in a given market to ensure fair competition), there is **no one-size-fits-all solution** on how to implement data access obligations in practice.

Still, we consider the following criteria as a basis for any future set-up of **mandatory data access for large online gatekeepers** in a given market.

Types of Data:

While the sharing of **personal data** has clear limits set out by the existing European data protection regime, it should not be entirely ruled out from falling under data access obligations. Existing case-law[7] and sectorial regulation have shown that the obligation of a company to share personal data with a competitor is indeed possible, as long as additional safeguards to guarantee data protection compliance are in place, e.g. prior consent of the user concerned or another available legal basis for processing.

While the granting of access to **non-personal data** would thus be less challenging to implement in practice, it might also be less effective: depending on the specific market characteristics, granting access to non-personal or anonymised data might not be sufficient to safeguard competition.

Categories of data:

Where data is generated through analytical efforts (**inferred** or **derived** data), e.g. by combining different datasets or using algorithms to create additional insights on user behaviour, the obligation to share such data could possibly infringe a company's IPR. In such a case, it could be difficult to argue that such data should be subject to access obligations. When no IPRs exist, obligations to share data could be imposed.

Similar legal barriers do not usually exist regarding **volunteered** (directly provided by the user) and **observed data** (e.g. telematics, observed online usage behavior). Therefore, an obligation to grant access to such data could be envisaged, as when it is oftentimes considered to be essential to compete in a given market. Such data should not only be provided in raw format, but be **structured** and **machine-readable**, to allow for carrying out data analysis without incurring in technical barriers.

***Portability/Interoperability*:**

While **data portability** already exists under Article 20 of the General Data Protection Regulation (GDPR), its scope is limited to specific cases under which the data subject can port its personal data to e.g. a competing service provider. This right does however not foresee continued and far-reaching access possibilities to different categories of data but is instead limited to receive the data "provided" by the user, to avoid lock-in effects for individuals.

In order to guarantee that competitors are also able to e.g. offer a complementary service, such data needs to be interoperable and thus able to be accessed based on a common standard and through the provision of an access architecture, e.g. via Application Program Interfaces (APIs). The technical compatibility of systems (i.e., **protocol interoperability**) to allow data transfers from one supplier to its access seeking competitors is thereby a pre-condition for the proper functioning of mandated data sharing in practice.

[7] See French competition authority decision GDF Suez, where access to personal data has been imposed subject to prior information and opt-out rights, https://www.autoritedelaconcurrence.fr/fr/liste-des-decisions-et-avis

European Cloud Ecosystem

As also highlighted by the Data Strategy, Europe is competitive when it comes to generating industrial data, e.g. in areas such as IoT and mechanical engineering. However, data storage, use and analytics are still mainly carried out by non-EU players, based on a **cloud infrastructure** that is largely dominated by only a few companies from the US and China.

Not only this **dependency** leads to a competitive imbalance and a loss of investment potential, but it also creates vulnerabilities to the security and protection of European data. Third country legislation in recent years have raised concerns in this respect. Furthermore, the COVID-19 crisis has shown that the lack of a European cloud infrastructure and cloud applications can subject the functioning of European essential services – and even the economy – to the priorities set by foreign cloud giants.

However, building a European public cloud that guarantees adequate protection to the data is a big challenge, due to the high level of technical complexity and sparse preparedness of a Union that is far behind China and the United States. The issue is not only a technological one, it is a legal one and it is also related to the broader ecosystem. Today's public clouds have attracted hundreds of thousands of software developers, distribution companies, and services.

Given the difficulties of creating a new cloud ecosystem from scratch, efforts should be focused on building a strong EU cloud market, including through a **pan-EU interconnected "cloud federation"** that could become the underlying digital infrastructure for the European data spaces and could reduce Europe's existing technological dependencies in this area. This project is a clear example of the much-needed European industrial policy and will help achieve long-term data sovereignty goals.

While recognising the right to choose different partnership models, we specifically welcome the Commission's aim to foster synergies with existing initiatives in this field such as **Gaia-X**, since the goal is the same: building an open, trustworthy and value-based infrastructure ecosystem in the EU, which facilitate the sharing of data among businesses while guaranteeing data sovereignty based on and in compliance with European values.

The concept of a European cloud federation should thus serve two purposes: (1) interconnecting the already existing server capabilities of European companies of all sizes based, where appropriate, on an open technology approach, to build a competitive, secure and trusted data infrastructure than can boost innovation; and (2) aiming for data sovereignty by setting up a data sharing architecture on top of this infrastructure that facilitates the control and use of data based on clear framework conditions.

The intended launch of a **cloud-based services marketplace** can support these goals by providing European businesses access to bundled data for driving projects in e.g. AI and Industry 4.0, thus driving scale and innovation.

To make this project a success, European governments and the public sector need to be fully committed to the initiative by generating initial **public demand**. This could imply that the future EU cloud architecture could be promoted in public tenders for data, government services and cross-border data exchange.

With regards to **funding**, building the cloud federation (being it under instruments like CEF 2 or Digital Europe programme), needs to be combined with the objective of improving terabit connectivity for High Performance Computing throughout the Union, due to the synergies between both objectives which are closely interlinked. Funding separate projects would undermine the synergetic effects.

Finally, concerning telco edge cloud platforms developed to deliver high performance for 5G networks, i.e. optimise latency or storage, we consider that the Commission should promote and encourage the emergence of this distinct alternative to hyperscale computing, also based on local solutions while preserving freedom of contract.

The goal of acquiring technological or digital sovereignty is to protect the **'European way of life'**, which means an open, democratic society that respects citizens in providing services to them. The EU needs to ensure that data stored in Europe adhere to European legislation, European rules, and the European way of life.

Policy contacts:
Paolo Grassia, Director of Public Policy
grassia@etno.eu