BUSINESSEUROPE

POSITION PAPER

Date (01/09/2022)

The proposal for a Data Act

KEY MESSAGES

1. BusinessEurope sees the potential of the Data Act proposal to enable new business opportunities. The new rules must be developed without creating excessive burdens for companies, especially SMEs; and give due consideration to industry's exposure to global developments.

2. The proposal's cornerstone definition of "data" must be aligned with Recital 17 and be compatible with the existing data-related legislation.

3. Business-to-business data-sharing culture relies on reciprocity, legal certainty for return of investments, the appropriate protection of trade secrets, sensitive commercial information, and databases. The Data Act must give a further boost to this data-sharing culture by preserving the contractual freedom businesses enjoy, by providing for adequate compensation for making data available and by ensuring clear enforceable obligations for third parties receiving data.

4. Business-to-government data sharing must be carefully balanced with democratic rights and democratic accountability. The proposal must narrow down the "exceptional need" situations, which would entitle many public sector bodies across the Union to claim data access, and ensure effective scrutiny.

5. The Data Act must promote the freedom of providers of data processing services and that of users to engage in contracts appropriate to the specific needs, as well as the wider adoption of codes of conduct for facilitating switching of cloud services and porting of data.

BUSINESSEUROPE a.i.s.b.l.
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL main@businesseurope.eu
WWW.BUSINESSEUROPE.EU – Follow us on Twitter @BUSINESSEUROPE
EU Transparency register 3978240953-79

CONTEXT

In view of the increasing digitalisation of EU industry, BusinessEurope agrees with the underlying principle that the multiplication of data, their availability and interoperability would lead to a multiplication of visible patterns fuelling more innovative data-driven products, processes, services and solutions. This potential should be harnessed to enable growth, increase Europe's competitiveness and its ability to address the challenges and opportunities of the twin (digital and green) transition.

- As a horizontal legislation the Data Act will impact the entire data economy. The regulation will lead to sharing and storage of data on a significantly greater scale, which will bring optimisation and efficiencies for the economic actors but could also entail increased energy consumption and cybersecurity risks.

- In an industrial setting, a recent study shows that up to 50% of factories' equipment on the production line might need to be replaced to enable deployment of IoT solutions at scale[1]. It is therefore essential to keep rules proportionate and ensure consistency with the regulatory framework in order to reduce cost of compliance and encourage uptake of data intensive solutions.

- The Commission points out in its impact assessment[2] that by 2030, the services and products linked to the IoT could enable $5.5 trillion to $12.6 trillion in value globally. We highlight that it is essential to keep the cost-benefit perspective and overcome[3] the difficulties to quantify cost and gains, thus allowing for informed regulatory and business decisions.

- OECD research suggests that data-driven innovation and data analytics investments lead companies to faster productivity growth by approximately 5% to 10% in comparison to companies that do not invest in data-driven solutions[4]. To exploit the full potential of the data economy it is key that the regulatory intervention at EU level creates a competitive and transparent digital environment, able to adapt to the rapid transformation of digital technologies as well as to promote and attract investments in innovation.

- Further investments should be devoted to the training of the workforce and to increase data literacy and data analytics, as skilled professionals are the main factors making Europe's data economy globally competitive.

[1] WEF & McKinsey & Company; (2019). *White Paper: "Fourth Industrial Revolution Beacons of Technology and Innovation in Manufacturing"*
[2] European Commission (2022), Impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)
[3] ibid
[4] OECD (2015). *Data-driven innovation: big data for growth and well-being*, Paris.

As a social partner and a representative of 40 national industry federations, BusinessEurope outlines its reaction to the Commission's proposal for the Data Act, below:

COMMENTS

Policy objective

With this legislation, the intention of the European Commission was to enable European businesses to catch *"the wave of industrial data"* that will define the winners in the next phase of the data economy. Further clarification however is needed as to why business-to-consumer (B2C) and business-to-business (B2B) data access and sharing obligations have been combined within the same legal act. While there are some products and services that can be used in both B2B and B2C settings, generally Industrial IoT and Consumer IoT require different safeguards as the amount and the nature of data generated are different. To introduce more clarity, it would help that B2B and B2C data sharing provisions are separated into distinct chapters thus allowing for more tailored regulatory action.

1. Scope and definitions

BusinessEurope underlines that clear and consistent definitions are essential for legal certainty, proper enforcement, and for further enabling of the business opportunities stemming from this piece of legislation. In addition, there is a need for greater clarity as to where the Data Act's applicability ends, and (existing and future) sectoral legislation begins. The Data Act must hold a carefully balanced position, which provides opportunities for businesses, and avoids unintended consequences amounting to access to market barriers.

DEFINITION OF DATA AND LINKS TO GDPR AND TRADE SECRETS DIRECTIVE

To help business predictability, effective enforcement, and compliance with the law, BusinessEurope argues that there is a need to achieve greater **consistency between the Data Act and the GDPR** and to refine several of the definitions in Article 2. **The definition of "data" is very broad and could create legal difficulties and an overlap of legal obligations,** on one the hand in handling mixed data sets of personal and non-personal data, and on the other hand in handling raw and inferred data. Recital 17 provides clarification that only raw data is in scope of the proposal ("data in the form and format in which they are generated"), which should be added in the main article. In addition, for the purpose of **clarifying the relation to Trade Secrets Directive**, it is not clear if *data* and *information* should be considered synonymous or not.

In relation to this, data portability must be looked through the lens of technical feasibility and what is the scope of data to be collected. Hence, a clear description of the content and scope of non-personal data would also help

compliance with the obligations set forth in the Data Act. A possible solution could be the adoption of codes of conduct for data portability and also creating synergies between the different policies for digitalisation of industry at all levels with an objective, inter alia, to help SMEs in understanding how to benefit by engaging in data sharing agreements.

DATA AND PRODUCT SECURITY

The Data Act obliges businesses to share data with third parties, pointed by the user. In some instances, those third parties might obtain data that could be critical to the integrity and security of a product or a service. While the intention of the proposal certainly is not to lower the requirements for security and safety of products and services set forth in other EU legislation, greater legal consistency and guidance is needed to ensure maximum compliance. Where appropriate, the data holder should be allowed to withhold sharing such critical data from a third party while also informing the user for such a decision.

In addition, it must be made clear how the data minimisation principle of the GDPR will be reconciled with the obligation to make data available to a user (who may not necessarily be the data subject) under the Data Act. The opinion[5] of the European Data Protection Board has also expressed concern in this direction.

OTHER DEFINITIONS

The definition of **"data holder"** also poses challenges for interpretation. While in Article 2(6), a data holder for non-personal data is understood as any entity that has the technical ability to make data available (which could potentially include several entities), **recital 24 equates data holders processing personal data to data controllers**. There is no explanation of why there is such differentiation between the mechanisms applying to personal and non-personal data sharing. **We believe that the same type of criteria should apply to personal and to non-personal data, and that a clearly defined entity (the data controller) should be responsible to act as the data holder.**

It remains unclear which components (e.g. sensors) of a physical asset fall under the definition of a "**product**". Furthermore, in the absence of a clear definition of a **"product that competes"** (referred in Art.6(2)), it is undetermined when a new product competes with a product from which the accessed data originated. Objective criteria need to be included for the parties to determine whether a new product competes with the existing product or not. The proposal could also specify whether the original product as a whole is meant or parts of such product. Furthermore, if the understanding is limited only to physical products, then the Data Act poses a risk that software or service providers could benefit indirectly by developing software-driven products/services based on the extracted data, which then compete directly with the original product/service.

[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)

The definition of a "**related service**" needs to address the responsibilities in the supply chain and who is best placed to provide the access to data. The proposal is also referring to "**consumers**", but a definition in Article 2 is missing. In addition, a definition for **"operator of a data space"**, will enable the enforcement of Article 28 by clarifying that it only applies to operators of data spaces of the Common European Data Spaces.

MICRO AND SMALL BUSINESSES IN THE DATA ECONOMY

Article 7 exempts micro and small enterprises from the obligation to share data in a B2B or B2C environment. In the digital economy however, the amount of data or the usefulness of data in a value chain do not necessarily depend on the size of a company. What if a smaller enterprise holds data, which accessibility could be crucial for unlocking innovation? Therefore, the Data Act must incentivise smaller players to participate in the data economy, for example through providing guidance and training schemes for interested smaller businesses.

2. B2B and B2C data sharing

BusinessEurope has consistently advocated for business-to-business data sharing based on voluntary and commercially viable collaboration between enterprises. The results of the public consultation for the Data Act found that 68% of the stakeholders who took part in it confirmed that they already share data with other companies. The Data Act has the potential to further enhance this data sharing culture by strengthening the legal certainty for the business community. This way the business would continue investing in the creation of smart products and services, more data generation, more accurate data analytics, and innovative data processing capabilities thereof.

TECHNICAL FEASIBILITY OF OBLIGATIONS

As a horizontal legislation the Data Act will apply to many data holders, different in sectors and in maturity. Therefore, the obligations for data holders must be technically feasible. In Article 3(2)a, the seller, renter, or lessor must provide the user with information on the nature and the volume of data likely to be generated. While there could be expectations of the nature of the data to be generated, the volume of data generation is highly subjective to the use of a product or a service, therefore BusinessEurope would suggest deleting the "volume" requirement from the paragraph.

The proposal should provide for the operationalization of the data access possibilities. There are no provisions on the need to develop secure access and transfer mechanisms, secure channels of communication, confidentiality, and obtaining consent. Article 3(1) must clarify the meaning of "easily" and "appropriate", especially as these requirements will extend across various industries. In this regard, it must be taken into consideration that costs for developing data accessibility/data sharing feature could be lower than redesigning the entire product.

LAWFUL DISCLOSURE OF TRADE SECRETS

Legal certainty, as regards to the protection of the confidentiality of trade secrets and commercial confidential information is essential for the business community. The Data Act does not contain any protections for commercial confidential information. From the point of view of fair competition, it is essential that the Data Act proposal does not lead to an obligation to share trade secrets. It can be detrimental for the data holder to forcefully disclose secrets with an entity (potentially unknown/unverified), or even several entities if the user so requests. This uncertainty may have a chilling effect on investments and business growth. Modal contracts can be considered an appropriate instrument to ensure both data sharing and confidentiality protection, in this regard including relevant language in modal contracts under Article 34 becomes crucial. However, in the event where the data recipient is an individual it is difficult to foresee how confidentiality can be preserved and what would be the means of the data holder to enforce it.

Considering the objective of the Data Act to foster data sharing and the harmonised protection provided by the Trade Secrets Directive aimed at increasing the incentives for businesses to undertake innovation-related cross-border economic activity (including research cooperation or production cooperation with partners, outsourcing or investment in other Member States), **BusinessEurope believes it will be important to ensure the proper application of the Trade Secrets Directive to regulate the lawful disclosure of trade secret information and data related to it as well as to provide adequate safeguards.**

RELATIONS WITH THIRD PARTIES AUTHORISED TO RECEIVE DATA

The Data Act aims at opening access to data to enable innovation in IoT services generally and to boost the proliferation of aftermarket services for IoT and innovative smart products. To this end, **co-legislators must provide effective control mechanisms at the disposal of the data holders so the latter can adequately ensure provisions in Articles 5 and 6 are respected.** For example, Article 5(5) clearly prohibits the use of non-personal data by the data holder to obtain information about the economic situation of a third party, but there is no equivalent prohibition for a third party in Article 6.

We strongly support Article 6(2)e, which prohibits the use of data for the development of a competing product by the third party or to share it to (another) third party. However, there is still a risk that the data can be used to obtain knowledge to compete against the data holder. Access to data between the entities should be carefully assessed to exclude the risk of distortion of competition: digital services are not just downstream services but are increasingly becoming the focus of the performance and value proposition in industrial applications. A flow of data from aftermarket service providers to product manufacturers could alleviate such concerns and help increase the reciprocity in data sharing and the collaboration among businesses, that ultimately will provide better value for the users.

Furthermore, to be able to use the economic potential of anonymized data and at the same time maintain the high level of data protection, we believe that legally secure and operational specifications for data-protection-compliant anonymization of personal data are of key importance and must be provided.

An important element to be considered when users share data with third parties is the security of users' data. A data holder duly exercising the obligation to provide access to data upon request by the user shall not be expected to know in what kind of environment the third party will process the data. The third party shall bear the responsibility to ensure the protection and security of the received data.

The proposal does not indicate how the legitimate interests of data holders would be protected in the event of unlawful use by third parties or how the data holder would even be aware of this. It appears that the burden of proof if an abuse took place, would be on the original data holder, which may be practically difficult and unnecessarily burdensome. From the outset, the data recipient should always be transparent to the user and the data holder about how the data will be used.

To strengthen the positive cooperation between data holders and data recipients, and avoid the risk of abuse, data recipients should question the conditions under which the data is made available, when they have a "reasonable doubt" and not when they "consider" the conditions discriminatory in Article 8(3).

COMPENSATION

The Data Act rightly allows for the data holders to make data available to data recipients under **reasonable compensation**. Such reasonable compensation should as a minimum cover the actual cost of making the data available, so that the incentives to develop innovative smart products remain. Paragraph 3 in Article 9 should detail under what conditions data holders can be obliged to share data with data recipients at a price lower than the actual cost or free of charge. This is necessary to ensure that the possible elimination or reduction of compensation does not preclude the even enforcement of the Data Act across the Union. Legal certainty is key for a predictable business environment.

Article 9 only caters for SMEs as a data recipient but does not cater for SMEs when it acts as a data holder. Hence, if Article 9 becomes a law as it is written, it seems that it will restrict the ability of an SME that is a data holder to calculate profit when it makes data available to another SME as a data recipient. Hence, it could be specified that paragraph 2 of article 9 applies only if the data recipient is an SME and the data holder is a large company.

The obligation to make data available for free could lead to a higher price of products and services, as expectations of securing revenue in an aftermarket service provided by the data holder will be lower, which in turn would lead to less money to be invested back into data innovation.

DISPUTE SETTLEMENT

The mechanism in **Article 10** can be further improved by including a provision on avoiding conflict of interest in paragraph 2. Paragraphs 5 and 9 should clarify if the parties can go directly to court or if they are obliged to go through a dispute settlement body as a first step. There is no clarity on what happens if a user is requesting data to be made available, while there is an ongoing dispute between the data holders and the data recipients.

SUI GENERIS RIGHT

BusinessEurope supports that the principle of *sui generis right* (Article 7 of the Database Directive) should not hamper B2B data sharing. The protection of databases granted under the Database Directive must not be lowered. To achieve this, there are some elements to be addressed: while the Commission's intention appears to be to unlock the data generated as by-product of the functioning of connected objects or related services, Recital 84 of Data Act provides clarification that sui generis right cannot be claimed for machine-generated data where it does not qualify for protection. In other words, if the maker of the machine-generated database can prove that there have been substantial investments in either the obtaining, verification, or presentation of the contents of the database, then the protection could be granted. Achieving B2B data sharing while protecting the database is key to developing a fair and competitive data economy. For this reason and to ensure legal consistency, Recital 84 and Article 35 of the Data Act should be aligned in order to reflect both needs for data sharing and database protection.

3. Unfair contractual terms

BusinessEurope welcomes the efforts to provide SMEs with the necessary tools to tackle potential unfair contract terms in the data economy. At the same time, we caution against any legal conflict with the enforcement of existing EU rules regulating contracts or national rules in B2B contractual fairness. The legislative gap that the Data Act proposal seems to be addressing is only regarding contract terms related to **access, use and data obligations** as specified in Article 13(1). Therefore, it is of paramount importance that this clarification is kept throughout the negotiation process and **Chapter IV's scope is not extended to other situations, beyond the data economy. This would aid the proper enforcement and prevent overlaps.**

It would be helpful if co-legislators introduce more clarity when a term "grossly deviates" from the "good commercial practice" by providing what negative outcomes are to be avoided. Equally important is the clarity on who would determine the deviation.

The proposal stipulates that the data holder bears the burden of proof to show that its terms are non-discriminatory and that they were not unilaterally imposed. This creates a situation "guilty until proven innocent", i.e. the party that supplied a contractual term must disprove the allegations made by the other party. In relation to Article 13(5) BusinessEurope suggests that both parties should be able to provide evidence to resolve these conflict situations, and for

the enterprises to prove that the terms are reasonable ("innocent until proven guilty").

Businesses must continue to enjoy the contractual freedom and to decide how data sharing should take place, what underlying solutions are used, how to adapt to the business models of the contracting parties, etc. This seems to be the rationale in Recital 54, which must not be watered down.

4. B2G data sharing

A thriving data economy is not possible if it is only limited to business-to-business and business-to-consumer data sharing avenues. Public sector also holds a range of data, which if paired with data held by businesses can provide for innovative solutions to socio-economic challenges. For instance, data generated by public bodies on statistics, demographics, public transport, meteorology etc. data may lead to further enhancing of existing activities, and more resource efficient provision of public services. There are already existing EU laws that govern the government-to-business data sharing, such as the Open Data Directive and the Data Governance Act. **Their impact however, on the data sharing culture, the data processing capabilities, and skills of the public sector is still to be determined.** However, the rationale for opening public sector body data in the above-mentioned legislation is because data are generated by publicly funded entities and should be available for the common good. It is less clear why that rationale should apply to private sector data.

BusinessEurope highlights that during the recent years, businesses have demonstrated that they actively engage in data sharing projects with authorities in order to mitigate the negative consequences of crises and help economies recover. We therefore advocate the B2G data sharing provisions in Chapter 5 of the Data Act to be clarified. There is an urgent need to ensure a uniform understanding of the large number of public bodies entitled to claim data access throughout the Union. A clear distinction should be made between data access requested under Article 15(1)(a) and (1)(b) and Article 15 (1)(c). Aside from public emergencies (paragraphs 1(a) and 1(b), which are unforeseen), it is difficult to understand why paragraph 1(c) would merit bypassing legislative action and scrutiny to invoke access to data.

Requests from public sector bodies should always be directed to the data controller. Data processors should not be forced to share customer data without customer's consent. The obligation to make data available when there is an "**exceptional need**" as in Article 15(1)(c) is problematic, as the **scope of this circumstance can end up being widely interpreted and data access requests from the many public sector bodies using this legal ground could become the norm rather than the exception**. As a minimum, there should be an obligation for the public sector bodies, upon the request of the data holder, to demonstrate they have used all possible measures to obtain the data before using the mechanism of Article 15(1)(c). Furthermore, public sector bodies should not be allowed to use private sector data to compete with the private sector.

We welcome the detailed approach in Article 17 but paragraph d) ("concern, insofar as possible, non-personal data") requires a specific mention as it must

not result in bypassing the GDPR and allowing for unregulated personal data requests. Furthermore, public sector bodies should be obliged to provide transparency on all purposes (primary and secondary) on what the data will be used for and on who the recipients will be. Article 18 must also recognise the contractual obligations of data holders with the users in terms of privacy, intellectual property, and trade secret protection.

Public sector bodies must consider the **potential risks, including cybersecurity** ones, when they obtain access to the data. In order to be able to guarantee the protection data security on the company's side, the data availability periods of five or fifteen working days must be extended. The Data Act should also provide clarity on how data holders can seek remedy in disputes over use of data by a public sector body. This is very much relevant if the data are further shared under Article 21. Furthermore, Article 21 must include at least a criterion for considering which actors fall within the definition of research institutions and how these should handle the data with appropriate safeguards. We remind co-legislators that the GDPR provides several rights for data subjects, inter alia the right to object to data processing. Hence, Article 21 in the Data Act must be reconciled with the GDPR.

A penalty should be imposed on a public sector body for non-compliance with the requirements suggested in this section.

5. Cloud switching, interoperability, and international data access and transfers

Europe should support inclusive and competitive cloud infrastructure that empowers business users, and where no vendor lock-in practices exist. BusinessEurope supports the efforts leading to a more competitive market, through more informed cloud provider choices and the removal of unjustified limitations of the use of cloud services. Co-legislators must avoid a one-size-fits-all approach in Chapters 6, 7 and 8.

CLOUD SWITCHING

The provisions of switching and portability should be nuanced based on the type and scope of data and the complexity of the transition of data, digital assets, and applications. Regarding data portability for cloud switching, Codes of Conduct (e.g. SWIPO) are very good tools to achieve transparency of the contractual terms about data portability when signing cloud services contracts. A widespread adoption of codes of conduct would make it possible to limit legislative intervention on aspects that should be left to contractual freedom.

The **mandatory transition periods** provided in Article 24 paragraph 1(a) and (c) are not in line with the technical complexities. For instance, for migrating simple workloads from one provider to another, a maximum period of 30 days or up to 6 months might be feasible. However, for more complex transfers more time would be required. Also, cloud service providers may need more than 7 days to respond in detail as provided in Article 24(2). Extending such a period should be possible when there are valid reasons for it, and the contractual

agreements with customers in this regard should be taken into account. Providers and customers should have the flexibility to agree on terms and conditions, which are technically feasible and appropriate to the specific use cases. It must be noted that technical feasibility restrictions can also occur when there are shortages of adequately skilled staff on either side, and it can contribute to the inability of meeting the deadlines set in Chapter 6.

Another compliance challenge to cloud switching stems from the lack of a definition on "obstacle". When switching of providers is requested, the normal business practice involves discussions between customers and providers to agree on specific service level agreements that providers must comply with during the termination assistance phase (where providers help clients to migrate their workloads to another provider). Parties also know that business and service continuity is better guaranteed through collaboration between the service providers (both the originating and destination services providers) and the customer, rather than through shifting obligations on the originating provider.

In addition, it is not evident why Article 24(1)b contains obligation to port "at minimum" all (i) data imported by the customer at contract start; and (ii) all data and (iii) metadata created by the customer and by the use of the service. Such a broad scope would result in longer switching process, but also may not be technically possible given the destination service provider. Also, it must be considered to include an obligation for the originating provider to delete user data after the switching is complete.

Further clarity would be welcome on "**functional equivalence**" (Article 26) for the switching of data processing services and which provider carries the responsibility to ensure it. Important clarification on what functional equivalence should mean in Recital 72 needs to be imported in Article 26 ("**maintenance of a minimum level of functionality** of a service after switching and should be deemed technically feasible whenever both the originating and the destination data processing services cover (in part or in whole) the same service type"). It should not be expected from the originating provider to change the service (make investments) in order to achieve similarity with the destination provider, nor the originating provider should request changes of the service of the destination provider. Such expectations would mean a deep interference in the freedom to conduct business and in the definition of value proposition by the different services. This could discourage innovation and the ability to gain a competitive edge for businesses in Europe. The regulation should take into account that customers may decide to switch providers because they value other (new) functionalities more than the ones they get in their current contract, and therefore may not require the same functionalities. Clarity is needed so as to avoid that the 'functional equivalence' uncertainty becomes a barrier to switching.

INTERNATIONAL ACCESS AND TRANSFER

While the Data Act Article 27 regulating international access and transfer of non-personal data mirrors Article 30 of the Data Governance Act, it should be noted that any guidance on non-personal data should be consistent with those

for personal data, given that often these types of data are stored together. However, Article 27(1) contains unclear and potentially disproportionate requirements. It must be clarified what would constitute acceptable "technical, legal and organisational measures, including contractual agreements" and how each supplier's actions would be assessed. The broad definition of "conflict" in Recital 77, could create impediments to companies' ability to transfer non-personal data. In practice, it is not the data processing service that knows whether the data is subject to trade secrets, IPRs, national security schemes or other Union or Member State law, but it is the data subject/the customer who has that knowledge.

A general concern is that SMEs will be put under obligation, essentially to perform investigations on the laws of a third country, which even large enterprises find challenging both when it comes to compliance costs and business opportunities. The absence of international agreement is evidence that the judgement whether third country laws are appropriate was not possible to be made by the relevant public bodies, which were tasked to do it. How could businesses be more equipped? Hence, businesses cannot and should not be expected to do a public function.

While Article 27 is not intended to limit data transfers, the lack of clarity risks discouraging customers from using global services that they would need or simply prefer. Concerns about data transfers and foreign government access to data are better addressed through multilateral solutions, which focus on common principles shared by countries, in order to promote regulatory dialogue, compatibility of requirements and ease enforcement and compliance. In this regards, co-legislators must clarify the intended purpose of Article 27, and how it advances the objectives of the Data Act to increase access to data, interoperability and data sharing.

BusinessEurope supports transparency requirements for data processing services in order to increase trust in the market, and in this regard supports Article 27(5). It should also be noted that governments must also abide by rules of transparency of requests. We remind that there is an ongoing OECD work stream aimed at resolving issues around trusted government access to data, which is suitable international format to establish common practices in such global industry as the data economy.

INTEROPERABILITY

BusinessEurope advocates for a bottom-up industry-driven transparent approach to standardisation that will bring greater interoperability. We welcome the ambition of the proposal to enhance interoperability under Chapter 8. We call for the **involvement of industry in the standardisation process.** There are positive examples of market driven initiatives in favour of greater interoperability, inter alia, the world language of production based on OPC UA technology, which was developed in the field of mechanical and plant engineering.

The Data Act must build on existing standards from ISO/IEC and other leading international standards bodies to facilitate multi-sectoral, cross-border and

international flows of data. The Commission must observe that standards adopted do not generate excessive implementation costs for the economic players concerned. In this respect, the requirements for smart contracts as proposed in Article 30, could result in an additional layer of administrative burden since smart contracts require close interconnection between the parties involved and tailoring of the smart contract could be necessary on top of the standard smart contract (Article 30(5) and (6)).

6. Enforcement and Entry into force

BusinessEurope strongly favours harmonised enforcing of rules as this is of paramount importance for the smooth functioning of the single market. **We believe that there is a need to streamline the approach in Chapter 9.** We would caution against the establishment of new competent authorities, and rather advise that Member States should rely on existing authorities to the maximum extent possible. There must be a coordinated approach between competent authorities in each Member States, similar to the approach established by the European Competition Network ECN+. The fact that enforcement and fines for non-compliance are split among different competent authorities in Member States poses the risk that rules will be diverging from one country or region to another, which would be detrimental to the Internal Market and discourage growth. BusinessEurope believes that, instead of fines, incentives and open dialogue between authorities and businesses should be at the heart of the Data Act enforcement. Furthermore, sector-specific legislation that is expected to come after the Data Act should not create imbalances in sectors, as this would prevent businesses from competing on equal footing.

Considering the number of the new obligations for data holders proposed in the Data Act, **twelve months will be extremely insufficient period** to implement all necessary changes, therefore the period **in Article 42 must be extended to at least twenty-four months.**