BUSINESSEUROPE

POSITION PAPER

9 November 2016

TOWARDS A EUROPEAN DATA ECONOMY

KEY MESSAGES

1 Digitalisation can be at the heart of Europe. The EU must timely complete the Digital Single Market, ensuring **free movement of data** to take full advantage of the digital transformation and compete effectively worldwide.

2 **The data economy is paving the way for the ongoing industrial revolution**. Its evolution can significantly improve lives, create growth and jobs, and benefit society overall.

3 Europe needs to adopt **an innovation-friendly approach to data** to empower the digitalisation process and offer robust solutions for data use. Policy makers should carefully assess if and where action is needed.

4 The European legislative framework for data must allow companies to compete globally, foster the creation of new business models and ensure a level playing field, with legal certainty and stability.

WHAT DOES BUSINESSEUROPE AIM FOR?

- **Data ownership, access and liability issues are adequately addressed by existing legislation**. Current rules and practices allow adapting to the needs of the parties and provide the appropriate setting to share data based on contractual terms, allowing innovation.

- The current framework is fit to address liability issues in the field of IoT and **no new liability rules for data-related services and products are needed**. Adapted or dedicated liability rules could be however required, in specific situations for completely autonomous systems.

- **EU legislative action to remove restrictions to the free flow of data is needed.** The ability to transfer data across borders is crucial for companies, both within the Single Market and beyond. Any forced data localisation requirements should be subject **to EU scrutiny and should only be kept if proportionate and in line with EU legislation and single market principles**.

KEY FACTS AND FIGURES

EUR 566 billion	Expected value of the data economy by 2020
41% of EU enterprises	Making no use at all of digital technologies
EUR 3.4 to 9.8 trillion/year	IoT market's expected economic impact until 2025 = about 11 % of world economy in 2025

BUSINESSEUROPE

POSITION PAPER

9 November 2016

TOWARDS A EUROPEAN DATA ECONOMY

1. INTRODUCTION

Digital is borderless by definition and allows real-time connections between countries, companies, objects and citizens. Digital can be at the heart of Europe but only if the EU triggers a real digital transformation and brings forward globally competitive propositions via distinctive innovation. In order to take full advantage of the digital transformation and compete effectively worldwide, the EU must timely complete the European Digital Single Market, ensuring free movement of goods, people, services, capital and data. This will allow and encourage individuals and businesses to seamlessly transfer, access and exercise online activities, ultimately defining a new scenario for doing business in Europe.

The data economy and related activities are paving the way for the ongoing industrial revolution. Existing players will improve and enrich their service offerings, and new players will enter the market by making use of the availability of data. The European Commission notes the data economy has the potential to reach EUR 566 billion by 2020. Besides the purely economic benefits, critical infrastructure can also be improved with vast benefits to society.

However, figures show that a very limited number of companies have developed a comprehensive investment strategy to grasp the potential of digitalisation. The use of advanced digital technologies such as mobile solutions, social media, cloud computing and big data is low, with 1.7% of EU enterprises making full use, and 41% no use. This issue needs to be addressed, because all companies – of any size and in any sectors – can benefit from digitalisation.

Digitalisation is still insufficient in particular for SMEs and in the less technologically advanced regions of Europe. Today, even the smallest firms can leverage the internet to compete with the largest multinationals. Reports show that approximately 12% of the global goods trade is conducted via international e-commerce, with surveys showing that even the smallest enterprises can be born global, with 86% of tech-based start-ups reporting some type of cross-border activity[1]. A recent report by the European Commission's Joint Research Centre shows that the negative impact of distance on trade costs matters four times less online[2]. This means that increased digitalisation could actually result in a more inclusive environment, in which SMEs can benefit from huge growth opportunities, no matter if they are located in more remote or traditionally less prosperous regions in Europe. As a result, it is key that all businesses independently of their scale or of the place they operate from are able and encouraged to grow and improve their efficiency and competitiveness thanks to digitalisation.

Digital technologies are delivering cross-sectoral efficiencies to business, including SMEs. The Internet of Things (IoT) is also a reality. The market for IoT components

[1] *Digital Globalization: The new era of global flows*, McKinsey Global institute, March 2016.
[2] *The drivers and impediments for Cross-border e-Commerce in the EU*, E. Gomez-Herrera, B. Martens and G. Turlea, JRC Technical Reports, 2013.

and systems has grown 160 % in 2013 and 2014, and is still expected to grow more than 30% in the next ten years. This can have a total potential economic impact of 3.4 to 9.8 trillion euros per year in 2025 (depending on the factors impacting on its development, such as declining technology costs and users' level of acceptance) and be equivalent to about 11 % of the world economy in 2025.

Big Data is closely linked to the development of Internet-of-things (IoT) activities such as the ability to aggregate data, to process it, make it accessible through cloud computing and to allow interaction in both a B2B and B2C context. Digital transformation is based on a growing ecosystem of advanced computing, data analytics, low-cost sensing and communication devices, new levels of connectivity, IT applications over the Internet, combined with business services know-how, that impact all value creation drivers and force companies in all sectors to rethink their business models. This means reduced costs and improved efficiencies, greater speed and scale, smarter products and services. Ultimately it enables first-time-right design and zero-defect, demand-driven production.

The evolution of the data economy has also created new business models, relationships between businesses and consumers, and sparked the attention of legislators. Certain EU Member States have put forward or discussed rules requiring - direct or indirectly - data to be held locally. Questions have also been raised concerning the value over data generated (both personal and non-personal), the ownership, access and use of such data, as well as how liability rules in this field should function.

Ultimately, the data economy's evolution has the potential to significantly improve lives, with substantial economic growth, social and environmental benefits, and job creation. The improvement of critical infrastructure for example will lead to safer transportation, better healthcare and better management of the planet's energy resources. It is crucial that any national and EU initiative facilitates – and does not stifle - these developments, and clarifies the applicable framework where needed.

Europe needs to adopt an innovation-friendly approach to data to empower the digitalisation process and offer robust solutions for smart and big data applications throughout value chains. Among other things, this also requires a balanced approach to the issue of **access for third parties to non-personal, machine-generated data**.

The ongoing digital transformation is mainly based on connectivity, collection and analysis of data, not necessarily personal data, but also non-personal/industrial data, for example data produced by machines. Today, businesses are using in most cases contractual solutions in order to address issues related to ownership, collection and processing of data. Clarity in roles and liabilities for the treatment of these data is crucial. In addition, it is important to recognise that different categories of data can be treated differently with different rules applying for their use.

The above does not automatically mean that legislation should be proposed (e.g. on new "data access rights"). Policy makers must refrain from rushing into regulation, but rather carefully assess if and where action or coordination at European level are needed to achieve a business- and innovation friendly legal framework for data use.

2. THE LEGAL FRAMEWORK

As Europe competes in a global market, the European legislative framework must allow companies to compete globally. It is important to analyse the current legal situation identifying where the gaps are and assessing whether the existing legal framework is fit to deal with new data based business models (including those where data and hardware are closely interlinked) in a way that allows solving potential conflicts arising in these new contexts.

Our regulatory framework, in particular concerning collection, use and analysis of personal and non-personal data, must empower the digitalisation process that will fuel growth in Europe. **Legislation must enable data-driven innovation.** A well-functioning, innovation- and business-friendly framework should deliver legal certainty, fair competition and allocation of rights and duties. It should also ensure consistent enforcement and a level playing field for all industry players across Member States, while at the same time foster consumer trust striking the right balance between **protecting EU citizens' rights and facilitating the free flow of data** in the single market.

Under a better regulation approach, the first reflex should be to **decrease regulation that is not needed and where it is not needed, and not to add new rules unless necessary, and based on proper impact assessment**.

For the moment, given the fast moving technological development and the emergence of new business models there does not seem to be an adequate case about the need for special regulation in this area. As the technical and economic developments cannot be foreseen, it is better to start with a principle and evidence-based approach, rather than specific regulation. At this point in time, in order to have a more innovative Europe, with a positive impact on growth and jobs, one should avoid creating new rules for every new innovative product or business model. At the same time, it is crucial to ensure that existing rules are effective, fast enough and properly enforced to meet the new challenges.

BusinessEurope believes that issues like data ownership, access and liability are adequately addressed by existing regulation. However, the situation needs to be constantly monitored. Regarding personal data in particular, the rights of individuals are extensively regulated by data protection rules, which have been recently finalised and are not going to be fully operational until 2018. The rights of access and use between commercial parties are best set by contractual relations.

Because of the wide definition of "personal data" under the GDPR, in certain cases it may be difficult to draw a line between personal and non-personal data. Still, we believe that to take advantage of the potential of data-driven economy, **different consideration should be given to personal and non-personal data**, as well as the industrial as opposed to the commercial internet, while still ensuring a level playing field among companies of all sizes, and from different Member States and sectors.

A starting point could be to incorporate privacy by design features to certain machines producing data – reflecting the type of process, the needs and the risks involved and avoiding a top-down, one-size fits-all approach as each business has different sets of data and applicable de-identification best practices will vary significantly. This would

allow transparency and control over what is collected and aggregated (and to whom it is disclosed).

The future framework should also provide clear incentives for pseudonymisation, as one of the possible tools to improve data security, and a means to significantly decrease the potential or perceived risks for data subjects. Where possible, data can be technically anonymised or pseudonomysed to facilitate and secure their usability. A consistent approach to **anonymisation** or optimal **de-identification** (where full anonymisation is not allowing any meaningful data flow) and **pseudonymisation** may offer robust solutions for smart and big data applications.

A balance must be found which meets compliance with privacy rules, ensures consumer trust and provides economic, environmental and social benefits.

3. Data Ownership, Access and Reuse

The European Commission is assessing whether action is needed concerning a framework for data access and ownership.

Currently, a legal concept of data ownership does not exist. The general practice is to establish agreements allowing controlling data streams and using the data to improve products and services, create new ones, and many more potentially endless aims. For the time being, this practice provides the flexibility needed to innovate and seems to work well. The introduction of entirely new and untested concepts could lead to unforeseen consequences. Restrictions placed on data ownership would not be justified and would have the potential to undermine the development and innovative data economy.

It is also key to carefully assess and define a balanced approach to the **access to data for third parties**, and particularly non-personal, machine-generated data. While openness is essential for the digital economy's development, it is also important to take into account negative developments potentially resulting from unlimited third-party access to data. Current contract law and practices allow adapting to the different needs of the contracting parties. Private sector is free to share its data based on contractual terms. It is of utmost importance that contractual freedom is maintained, otherwise innovation on big data will suffer dramatically, like for example from the perspective of who has already carried the burden of pre-investment costs. Any debate on potential legislation in this field on the question of data ownership has to be based on thorough analysis of pros and cons of any solution. Caution also applies to granting open access to research data from private-sector R&D or from public-sector research performed in collaboration or (co)financing with industry because this could potentially discourage industry from participating in such collaboration.

Existing EU legislation is well equipped to grant sufficient and fair access to and use of data, and safeguarding fundamental interests of the subjects involved. There is on the one hand widespread interest in ensuring broad and fair access to data held and/or aggregated for those who want to use it for commercial or public interest purposes, but it is also to ensure that (in particular smaller) companies should be able to valorise their data on fair terms vis-à-vis commercial partners in the data economy.

While data is different in that it's replicable, non-exclusive, readily available, the potential conflicts with regard to the use of data in the digital world are not entirely new: potential market power imbalances, access to essential facilities, consumer protection, legal clarity and certainty. As a consequence, the default approach should be to assess whether existing regulation is fit to solve these conflicts also in the digital world. These issues are adequately addressed by existing regulation including data protection, competition, unfair commercial practices, contract and consumer protection law, intellectual property laws, the database directive and the new trade secrets directive. When dealing with consumers-users, they also enjoy additional protection under the Consumer Rights Directive, the Sales Directive, the Unfair Contract Terms Directive, and the upcoming proposal on contract rules for sale of digital content.

There is a broad consensus within industry that legislative intervention is not necessary, that **the existing framework and contractual arrangements are satisfactory**. Regarding personal data in particular, where the rights of individuals are extensively regulated by the data protection rules, respondents noted that in absence of proof of market failure, existing legislation adequately deals with the issues of ownership, use and access.

The rights of access and use between commercial parties processing both personal and non-personal data should be set by contractual relations between the various parties involved. Contracts are widely used today, are flexible and can be adapted to emerging business models and new technologies. While do not believe there is a case for the creation of new compulsory access rights, we believe it is useful to assess whether the existing legal framework is fit to answer newly arising questions.

In the B2B context, the data accessed and used is usually defined through contracts between the involved companies or organisations. Given the disparate entities potentially involved in the offering and differences in the nature and purposes behind the generation of certain types of data, BusinessEurope as well as the majority of the respondents to the various Commission consultations, are not convinced that a uniform regulatory solution is preferable to existing contract negotiations.

In the B2C context, the data subject has the right under current and future data protection rules to transparency and control over their personal data. There are clear benefits, however, to sharing of this information in an aggregated and anonymised way, for example intelligent transport management for traffic flow predictors where the more traffic data that can be collected, the better the accuracy. Therefore, a balance must be found which meets current privacy rules, ensures consumer trust and provides economic, environmental and social benefits. This should be achieved by providing the right incentives to users for contributing to this kind of data. Overall, these types of data have a little or no privacy implications when they are aggregated and anonymised, while they may have tremendous benefits for the public.

Also, encouraging the use of the **Innovation Principle** is particularly relevant in this debate. Whenever legislation is under consideration, its impact on innovation should be assessed. This provides a timely reminder that legislation is needed to support innovation and encourage investment in new enabling technologies. We are confident that the innovation principle would complement the precautionary principle and existing risk management rules to encourage a balanced view of benefits and risks. In this context, the ability to innovate is based on the ability to invest – which requires the possibility to make use of data generated as a result of upfront investment.

4. LIABILITY

While IoT technologies create interdependencies between multiple product developers, service providers and users of the data, that is also true for other types of technology and services with complex supply and value chains. In this respect, the existing legal framework is fit to address liability issues in the field of IoT and we see no need for new liability rules for data driven services and connected products, especially not in the B2B area.

The Product Liability Directive (85/374/EC) imposes liability for damages caused by defective products on the producer. While its applicability to technologies that operate more as a service than 'traditional' products might need some additional elaboration, this is not a new issue and should be addressable under the existing framework.

However, Business Europe does recognize that in specific situations using completely autonomous systems, adapted or dedicated liability rules could be required. We therefore suggest an in depth analysis of the existing rules to specific use cases of autonomous systems so to determine if the existing legal framework is fit for purpose or if new rules or tools are required to address liability challenges

5. DATA LOCALISATION

The ability to transfer data is crucial for companies everywhere in the world, no matter their size or the geographic area where they operate. Data flows are an integral part of daily companies' operations, as well as international trade.

Companies need to be able to efficiently transfer data across borders in order to respond to customers' need, deliver goods and services to consumers, process payments or provide customer support. Imposing direct or indirect restrictions on the location of data, thus limiting the possibility of data flowing across borders without objective and justified reasons would undermine the ability of companies to define their business models and therefore be detrimental to competitiveness and growth of EU companies, while also endangering the functioning of critical infrastructure (i.e. medical devices). On the other hand, if they concern personal data, transfers must be carried out in accordance with the new GDPR, irrespective of the nature and location of the player, in order to guarantee a fair protection of users. If this is not the case, users will not be encouraged to use these new services, to the detriment of all parties.

BusinessEurope fully supports an EU legislative initiative specifically focusing on the removal of any restrictions to the free flow of data, while acknowledging that businesses have the right to choose where they store their own data. While companies' decisions on data location can be seen as a solution, or part of a business model for specific companies in specific sectors, and companies must be allowed to autonomously take decisions on data localisation, we strongly recommend avoiding any forced data localisation requirements on a national, European or global scale. In addition, Business Europe is concerned that in several cases public procurement contracts require local data storage and also would like to see this addressed.

These requirements in most cases find no valid justification, as there is no rationale behind the assumption that within Europe data are safer when stored in the territory of

a certain Member State over another. Also, forced localisation makes it more difficult to implement best practices in data security - including redundant geographic storage of data and the usage of distributed security solutions. In addition, under these requirements, companies must often increase reliance upon local data centres that might lack sufficient capacity, upgraded hardware, or experienced security personnel to counter intrusions and detect signals associated with potential breaches. While data centres can be replicated, teams of specialised data experts to be found in specific hubs cannot, meaning critical devices cannot be properly serviced if data is to be localised. This also implies that governments should work closely together to create a common space with a similar level of protection for data.

Businesses would be deprived from the ability to deploy the best technical measures available to protect security, only because they would have the obligation to store the data in a specific geographic area. Storing data in a single centralised location can also offer a more attractive target for hacking or surveillance, because the efforts to access or compromise one single data centre rather than several ones are limited.

Justifications put forward by Member States for such measures normally relate to overriding reasons of public interest, like national security and law enforcement. However, by looking at the business community's experience with the evolution of the single market, we notice that these possibilities are often used extensively by Member States, some of which tend to put forward unnecessarily protectionist/restrictive measures. Also, under a digital single market perspective there is little justification to deem data safer or better accessible by default if stored in a specific Member State, as the physical location where the data is stored does not seem to have much relevance anymore.

In light of the above, BusinessEurope would encourage the European Commission to consider the introduction of a **legal instrument that (1) removes existing laws requiring data localization within a certain territory, and (2) introduces a notification procedure that should ensure that extra national requirements are always notified and can only be kept if proportionate and in line with EU legislation and single market principles**. Under this notification system, Member States should be obliged to notify any new additional measure, legislative and non-legislative, and the **"burden of proof"** should be on national authorities to show these measures are needed and proportional to reach a certain (public interest) goal. Otherwise the national measures should be de facto considered void and should therefore not apply. This should be subject to a **"standstill clause"** during the time the Commission is assessing whether or not new national initiatives are in line with EU legislation and single market principles. The revised notification obligation/procedure should cover national requirements that directly or indirectly hamper the free flow of data, including data localisation requirements under public procurement tenders. Furthermore, a notification procedure should provide transparency about the notified requirements, as well as the comments and objections from other Member States and the Commission. This would be in line with the notification procedure for services announced by the Commission's 2016 Single Market Strategy.

* * *