BUSINESSEUROPE

POSITION PAPER

26 April 2017

BUILDING A EUROPEAN DATA ECONOMY

KEY MESSAGES

- 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.
- 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.
- 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	No using digital technologies at all
EUR 3.4 to 9.8 trillion/year	Year 2025: IoT market's expected economic impact until = ~ 11 % of world economy

BUSINESSEUROPE

POSITION PAPER

26 April 2017

BUILDING A EUROPEAN DATA ECONOMY

1. INTRODUCTION

BusinessEurope appreciates the opportunity to contribute to the debate on the European data economy through the consultation launched by the European Commission on 10 January with the publication of the Communication on Building a European Data Economy. We refer to our previous paper Towards a European Data Economy, published in November 2016 and our public statement "Free Flow of Data is at the essence of a true European Digital Single Market".

The data economy and related activities are paving the way for the ongoing industrial revolution. Existing players will enrich their offerings, and new players will enter the market by making use of data. The 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.

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 and capital. There should be no distinction between a Digital Single Market and the Single Market, and the latter is ultimately fundamentally weakened by data localisation measures, which undermine the very essence of the four freedoms. The success and growth of the European economy as a whole is hindered if data localisation measures are allowed to proliferate.

Digital technologies are delivering cross-sectoral efficiencies to business, including SMEs. The market for IoT components and systems has grown 160 % in 2013 and 2014, and is expected to grow more than 30% in the next ten years. This can have a 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.

But these results will only be achieved through a coordinated approach to the various policies that affect the digital economy, from privacy to innovation, IP, consumer and competition policies among many – and in particular the recognition that **a true *digital* single market cannot be seen separately from the physical single market**.

We support the overall Communication's premise that a well-functioning data economy requires the flow of data in the single market. This premise and the current situation in the Single Market concerning data localisation restrictions demonstrate the need for clear action as single market principles are being breached by some Member States. We strongly regret that the EU failed to enforce the free movement of data and facilitate data flows despite strong cross-stakeholder and Member States' support.

The current propositions will not solve the problem: infringement proceedings are highly political and take years to complete. The Commission indicates it "may also take further initiatives on the free flow of data", but without further details.

BusinessEurope believes EU legislation to remove restrictions to the free flow of data created by Member States is needed. Any forced national 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. Guidance on data storage justifications and increased transparency of restrictions imposed by Governments would also help.

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. It is crucial that any national and EU initiative facilitates – and does not stifle - these developments, and clarifies the applicable framework if needed.

Today, businesses are using in most cases contractual solutions in order to address issues related to ownership, collection and processing of data. It is important to recognise that different categories of data can be treated or regulated differently.

In light of the above, BusinessEurope would not support a possible EU framework for data access or the creation of 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. LOCALISATION OF DATA FOR STORAGE/PROCESSING PURPOSES

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 and trades and a catalyst for the proper functioning of the Single Market.

Increased digitalisation and data flows 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 to grow and improve their efficiency and competitiveness thanks to digitalisation and data flows.

As the Commission rightfully mentions in its Staff Working Document accompanying the Communication, the trend in Europe is towards more, not less data localisation (+100% in 10 years), which may also explain the general misconception among administrations and businesses that there actually is a legal obligation to store data.

In December 2016, BusinessEurope and other organisations adopted a joint statement highlighting the importance of free flow of data and listing examples of existing national localisation requirements.

As the Commission notes in the Communication, **data localisation measures effectively reintroduce digital border controls** which constrain the development of the EU data economy and fundamentally undermines the Single Market. Such protectionist measures prevent companies, especially European SMEs, from scaling-up and entering new markets. As a consequence, customers' access to state-of-the art technologies or cheaper services is limited, with a direct and negative impact on the uptake of cloud computing in Europe.

We must also address the **damaging misconceptions about data localisation**, which is sometimes wrongfully justified as assurance of stronger privacy and security. What matters in terms of security is how the data is stored, not where: the combination of state-of-the-art cloud computing together with modern cybersecurity tools and practices is the real enabler of secure storage and processing, rather than data

localisation. Data localisation measures actually weaken security as they make centralised data easier to target thus more vulnerable to attacks. Also, data localisation can endanger the security of organisations and institutions which operate cross-border, as they rely on global information systems and cybersecurity tools and teams.

Data localisation can actually weaken security and brings nothing but higher costs and fewer services to businesses and public administrations which need to store and process data in the Union.

Companies need to be able to efficiently transfer data across the single market in order to respond to customers' needs, deliver goods and services to consumers, process payments or provide customer support. Imposing direct or indirect restrictions on the location of data, thus limiting cross-border data flows 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. Privacy concerns are largely unfounded in the context of the Industrial Internet as it overwhelmingly relies on machine-to-machine communication of data necessary for the optimal operation of machines. The use of personal information often aims to make the machine work better, lower radiation or incidence of disease, or develop aggregate models of care. These data may be aggregated, allowing for its use for research without posing significant privacy risk to individuals. Also consumers generally do not interact directly with Industrial Internet devices and systems, that generally do not collect consumer data for marketing purposes. Personal information collected from Industrial Internet systems is used to improve machine or fleet efficiency, increase safety, and to secure networks, but not for deciding whether to market specific products or services to a particular consumer.

Removal of localisation requirements may reduce business costs, e.g. additional cost of local data storage. A 2016 study published by the European Centre for International Political Economy (ECIPE) found that costs of storing data may vary by up to 120% between the cheapest and most expensive Member States. Removing localisation requirements would enable companies to plan their data storage in a more cost-efficient manner, and **encourage competition in the European data storage market**.

A March 2016 report by the McKinsey Global Institute showed that approximately 86% of tech-based start-ups reported some type of cross-border activity. The technology industry thrives on cross-border business: restrictions that limit the ability of companies to expand into new Member State markets (i.e., rules requiring local data storage and, therefore, the cost of doing business there) create a disadvantageous environment for companies operating in Europe. This is not a tech-sector only issue, however; an increasingly expanding range of industries are dependent on data flows. Removing localisation restrictions would reduce barriers to entering certain markets, and increase European consumer choice as a result.

Imposing restrictions on the location of data limits their cross-border flows, which hampers innovative uses of data and prevents organisations from gaining insights and achieving advances that are possible only with extremely large datasets. Such restrictions also undermine the ability of companies to pursue business models based on optimal technical and commercial arrangements and thus harm the competitiveness and growth of EU companies: a constraint on the freedom to contract flexibly. The ability to transfer data across borders is crucial for EU companies to gain and maintain global leadership in data-driven innovation and growth. These innovations also hold

tremendous promise to benefit society, in areas as diverse as health, education, public services, energy conservation, and many others.

Conversely, confusion over localisation rules, and subsequent requests from customers, can inhibit innovative and socially beneficial uses of data and increase the cost of doing business unnecessarily, thereby preventing job growth and economic development in certain sectors**. If the EU legislative framework were fully enforced and more clearly restricting Member States from imposing data localisation requirements, this would enable the EU to compete globally more effectively**, foster the creation of new business models, and help ensure a level playing field, with legal certainty and stability.

BusinessEurope fully supports legislative initiatives specifically focusing on the removal of Member States' restrictions to the free flow of data in the EU, while acknowledging that businesses have the right to choose where they store their own data. While companies' decisions on data location can be part of a specific business model, and companies must be allowed to require or provide data localisation, that is a free choice for both providers and recipients of the service – which is entirely different from a legislation obligation to do so. In addition, BusinessEurope is concerned that in several cases public procurement contracts require local data storage and also would like to see this addressed.

These requirements by Member States 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 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 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 most cases (certainly in those involving non-personal data), there is no valid justification for data localisation. Member States' interests in national security and law enforcement are fully legitimate but are too often used to justify measures that in practice have no strong relationship to these interests. We agree with the Commission's statement in "Building a European Data Economy" that localisation restrictions rarely advance the public policy objectives they are intended to achieve.

In light of the above, BusinessEurope would encourage the European Commission to strictly enforce existing single market rules that can tackle barriers to free movement, and consider the introduction of a **legal instrument that (1) removes existing laws requiring data localisation 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.

3. DATA OWNERSHIP, ACCESS AND REUSE

The European Commission is assessing whether action is needed concerning a framework for data access and ownership. Understanding each actor's role within the data processing chain is key and the rights on data are set by the contractual or licensing framework combined with the regulatory framework for personal data. This is an area where change happens continuously and rapidly and clarity on these dynamics is needed before taking any action.

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. Data ownership restrictions would not be justified and would have the potential to undermine the development and innovative data economy. Also, a discussion involving all stakeholders on what constitutes public interest data should precede any further action.

The creation of a "**data producer's right**" has raised a lot of concerns during the various consultations organised recently. Not only would such a right limit the flexibility that is necessary for companies to define and agree on contracts, it would also be difficult to determine and apply in practice.

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.

From an investment perspective, it is crucial that businesses can use and protect their own (machine-generated) data as they see fit, to develop new products, find innovative solutions and get a return on investments. It is vital that legislation contributes to protect investments, intellectual property rights and trade secrets.

Contract law and practices currently 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. On the one hand, there is 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 on the other to ensure that (in particular smaller) companies are able to valorise their data on fair terms vis-à-vis commercial partners.

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. Such access should be negotiated through contracts rather than via legislation.

While data is different in that it's replicable, non-exclusive, readily available, the potential concerns with regard to the use of data in the digital world are not entirely new. As a consequence, the default approach should be to assess whether existing regulation is fit to solve these conflicts also in the digital world.

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 through rules on data protection, competition, unfair commercial practices, contract and consumer protection law, intellectual property laws, including the database directive and the new trade secrets directive. To the extent that the processing (including access, transfer and use) relates to personal data, which is very broadly defined in Europe, the rights of individuals are extensively regulated by data protection rules.

There is a broad consensus within industry that legislative intervention is not necessary and that **the existing framework and contractual arrangements are satisfactory**. BusinessEurope remains committed to continue being engaged in this discussion in view of potential future developments.

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.

We do not see any need for **mandatory default contract rules** which would quickly become obsolete and counterproductive. The Commission should in any case explain beforehand what exact types of market failure exist and which specific imbalances in negotiating powers have been reported. In any case, such potential imbalances should not be addressed via new legislation that might undermine or discourage contractual freedom and commercial negotiation.

We fail to see what a system whereby data holders would receive **remuneration in exchange for providing access to data** would bring, when compared to the current situation in the market. Today, data holders are free to decide if, how and with whom they want to share the data they own.

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. Data use and licensing practices are so diverse and complex across sectors that they are not susceptible to "one-size-fits-all" regulation. Also, in some scenarios, our members do not license data to others at all, such as where that data is commercially sensitive, private, or where it is unstructured and thus of little utility to third parties.

Not all of the actors involved in a 'system' will have equal claim to all types of data. Where additional analysis or combinations of data have been used to draw out new insights this is clearly added-value brought to the data by the processor in question. Even the customers who opt for a specific solution may not need access to all the data being generated. Some data may be business confidential, whereas in other cases they may decide they have limited interest in the data in question and may be willing to trade it against other advantages in contract negotiations. Without evidence that such negotiations are proving unworkable and that the current rules (e.g. on competition) are insufficient, we do not see a need for regulatory intervention.

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 format and the urge for an all-encompassing interpretation of the personal data definition should be balanced with these gains. For example, one must consider intelligent transport management which requires the collection of personal location data to map and predict traffic flow. Accuracy improves as more traffic data is connected.

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 proposal on contract rules for sale of digital content.

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 little or no privacy implications when they are aggregated and anonymised, while they may have tremendous benefits for the public.

Non-binding guidance based on existing legislation, on how non-personal data control rights could be addressed in contracts could be useful - if at all necessary – provided the objective is indeed to support companies in better understanding existing rules. Non-binding guidance to end users is also useful on the elements that users should expect to find in a services contract. The Commission's work on Service Level Agreements and the recent set of ISO templates and standards on SLAs constitute useful support in that regard.

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.

In the absence of any demonstrated market failure **it is clear that contractual relations**

and existing rules remain sufficient. It is premature to conclude that new legislation is needed, and we believe that market operators are best placed to decide which business models and contractual arrangements suit their needs. The existing rules should be carefully assessed according to various use cases, and soft regulation should be promoted.

We are committed to continue this debate in view of potential future developments.

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) currently under consultation 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.

Therefore, existing rules in the Products Liability Directive can apply to IoT devices. In addition, like many other business models, the Internet of Things relies on supply and value chains which can involve a great number of service providers and users. In all those business models and equally for data driven services and connected products, liability is assigned in contract terms which provide the necessary legal certainty for parties in the supply chain.

BusinessEurope does recognize that in specific situations using completely autonomous systems, adapted or dedicated liability rules could be required. We will participate to the ongoing public consultation carrying out an 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. Premature intervention should in any case be avoided unless specific concerns are identified.

While the existing legal framework on liability rules seems appropriate, we see value in the Commission's proposals in this Communication regarding "Experimentation and Testing", including for liability rules. We agree that testing in real life environments with the involvement of all stakeholders should precede any conclusions on liability. Experimentation and testing would also be appropriate regarding the development of fully-autonomous systems, which might benefit in the future from adapted liability rules.

The idea of assigning liability to market players "which are best placed to avoid the realisation of such risk" raises many questions and concerns. It is unclear who could impose such liability and which criteria would be used for this assignment. In our view, this should be left to contractual arrangements between parties in order to guarantee enough flexibility and adaption to each particular case.

Although a discussion on insurance schemes would be useful, imposing insurance schemes could also produce unexpected effects on businesses as it may imply that data economy services are particularly risky. It should be left to businesses to decide if and how they want to contract insurance schemes.

5. INTEROPERABILITY, PORTABILITY AND STANDARDS

Encouraging the interoperability of systems and data portability are objectives the Commission should pursue, notably by promoting the use and, if and where needed, facilitating the emergence of industry-led standards.

The development of IoT requires a certain level of interoperability. However, **mandating standard contract terms for interoperability and creating data portability rights are not suitable instruments to achieve these goals**. The best way to achieve them is through sector agreements and industry driven standards developed by businesses with extensive knowledge of how technology, contractual arrangements and business models work.

Interoperability is key to the functioning of the many services, infrastructures, and devices in the data economy. However, imposing the adoption of interoperable systems and models via government mandates generally does little to enhance competition and hinders innovation. Non-binding guidance and best practice on how to achieve interoperability, as well as possible voluntary industry initiatives, would be more appropriate. The main focus should remain with industry, and its efforts in the field of standardisation at global level.

Regarding data portability, we agree that users should be able to switch providers as easily as possible. Considering that vibrant competition in the various markets drives service providers to facilitate portability, we believe that data portability is a key issue and will be achieved via the adoption and, if needed, **further development of industry-led portability standards**, provided such standards have been developed openly and transparently and tested among a variety of vendors. It is furthermore important to reference global ICT technical specifications that have been developed in global fora/consortia following the same open and transparent processes.

Non-binding guidelines and best practices can be very useful in advising cloud users before the standards become available. As such, current discussions on **portability standards** should be supported in global standards bodies including fora/consortia. What would hamper innovation and technology adoption are contract terms requiring service providers to implement the portability of a customer's data.

We are not convinced that creating data portability rights is necessary or even advisable in the **B2B context**.

In a **B2C context**, the requirements on data portability in the General Data Protection Regulation are difficult to deal with for companies. Technically it requires that different companies apply the same data format in order for it to be portable. Rebuilding IT-solutions entails high costs and currently there are no guidelines for how companies are to handle this technically. Imposing similar demands on machine-generated data would mean enforcing a regimentation of technical solutions and IT-systems that would hardly benefit innovation and competitiveness in Europe.

6. CONCLUSION

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 in a way that allows solving potential conflicts arising in these new contexts.

Linked to the above is the conclusion that data localisation should not only be prohibited within Europe but also globally.

It is important to make the fundamental distinction between the industrial Internet and the consumer Internet because B2B machine-to-machine communication (e.g. of telemetry and similar data) does not require the same privacy interests as for individuals' data in a B2C context.

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. **Policy 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.

* * *