



5 January 2016

BUSINESSEUROPE Response to the public consultation on regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy

Introduction

The Digital Single Market must remain a priority for the EU over the next years. With a completed and fully functioning Digital Single Market, Europe can gain 4% of GDP by 2020. Digital is borderless by definition and allows real-time connections between countries, companies, objects and citizens. Digital can truly be at the heart of Europe's recovery, but only if the EU gives itself the means to trigger a real digital transformation. The EU must timely undertake the necessary actions to complete the Digital Single Market, ensuring free movement of goods, persons, services and capital and allowing individuals and businesses to seamlessly transfer, access and exercise online activities.

The collaborative economy and platforms are at the core of the digital transformation. Their importance for the digital economy is growing exponentially and will grow even more in the coming years. The right framework will further enhance the digital economy's strength in the creation of new businesses, jobs and improvement of current business strategies.

BUSINESSEUROPE would like to express its support to the Commission public consultation's attempt to first develop a broad understanding of any potential challenges related to platforms, cloud computing, online intermediaries and collaborative economy without rushing into proposing legislation or solutions.

This paper addresses the most relevant elements of the consultation for BUSINESSEUROPE. Some questions are tackled extensively, while others are left out. The paper indicates, whenever possible, the specific sections addressed in each section. However, the purpose of this document is also to be a self-standing paper presenting our views on the themes covered by the consultation.

General remarks

There are a number of common principles that we would like to highlight and which we believe are relevant for all of the issues analysed below. We would like to present them upfront in this this section.



While addressing challenges related to the data-driven economy, it is important to analyse the current legal situation identifying where the gaps are. Policy makers must refrain from rushing into regulation, but rather carefully assess if and where action or coordination at European level may be needed. For instance, action at EU level is needed particularly to avoid divergent approaches at national level, which are already creating fragmentation within the EU Single Market. Legislation should only be put forward where real gaps exist and on a case-by-case approach. Existing competition law can help addressing the digital economy needs. Precisely in light of the importance of the digital economy for the future of Europe, and since some of the relevant markets are evolving rapidly, policy makers should also **consider how antitrust policy could provide faster interpretation and guidance** against the backdrop of new developments to face new challenges, as a result of the way digital markets operate and to ensure timely intervention where needed.

Policy makers need to carefully assess potential unintended consequences of excessively strict regulation, which might prevent companies from having the ability to find innovative solutions, or apply best practices. Adopting too rigid rules would lead to less efficient solutions and not achieving the objectives in the optimal way (e.g. increased security). Any intervention should be targeted and fact-based. It is crucial to avoid disproportionate actions and unwelcome side-effects that could hamper innovation in a very dynamic and rapidly evolving space.

The digital economy is in constant and rapid evolution. It is key that any regulatory framework on the digital economy reflects the need for flexibility to adapt to this evolution, without stifling innovation and growth. It is important to avoid creating new rules for every new innovative product or business model.

Under a better regulation approach, the first reflex should be to review the need of existing regulatory obligations. The overall approach should always be to simplify and decrease regulation that is not needed – or not anymore – and, where it is needed, not to add new rules unless necessary.

Targeted regulation – if legislators would choose to move in this direction - can be very problematic, in particular for small companies. The consequences of possible new rules designed for targeting specific companies, sectors or business models would in all likelihood have broader and unintended spill-over effects into other companies and sectors, with a negative impact on jobs. This is particularly the case for smaller European businesses and start-ups, which have fewer resources to face an increased level of regulation. What only slows down larger businesses can knock down promising SMEs altogether.

Many of the topics addressed in this consultation touch upon several policy areas, such as competition, consumers legislation, employment, data protection, intellectual property and standardisation. The Commission must ensure that any specific legislation in these areas takes into account its impact on the European digital economy and is not in conflict with the objective of fostering the Digital Single Market.



Trust is key for digital development. Citizens' trust and their willingness to rely on digital solutions and services, combined with enabling conditions for companies to gather and use data, are crucial. This requires balanced regulation, education and change in mentalities.

Rules must be future-proof and reflect the rapidly changing nature of the digital world. Models and practices valid today might not be relevant anymore tomorrow. Therefore the legislation should not seek to anticipate or steer future developments or, worse, to stifle them. It is essential that any legislation reflects this reality, providing technology-neutral solutions which create a level playing field amongst players that offer the same service and avoid excessive regulatory burdens based on backward-looking approaches.

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.

1. ONLINE PLATFORMS

1.1 Definition and general observations

The notion of “digital platforms” is currently used to indicate different models, such as search engine services, operating systems and social networks. BUSINESSEUROPE notes that there is no common and clear-cut understanding of the concept of digital platforms. The Commission's attempt to formulate such a definition risks creating new legal concepts trying to encompass business-models, which are by nature, rapidly changing, and can create artificial boundaries, stifle innovation and undermine the development of new growth-enhancing business models. We therefore do not support this definition.

Platforms have existed since commerce began, with buyers and sellers being brought together by intermediaries in different markets. The ability to transform an offline platform to an online version increases its reach, but the concept remains fundamentally the same – connecting buyers and sellers. Some platforms operate in multi-sided market models where the offering is not provided against monetary compensation, thus transforming market dynamics. Some of them integrate different layers turning into platforms of platforms. Approaching the definition of what can be considered a “platform” should reflect these situations, and must consider the specific context in which the definition will apply.

1.2 Economic role of online platforms

Platforms have a beneficial economic role and are important engines of the digital marketplace. While different types of platforms provide different types of benefits, they facilitate information and communication, helping the matching of offer and demand in the Digital Single Market. Platforms allow consumers not only to buy online, but also to widely research on prices, offers, quality, comparison of products and consumers' experience, enabling them to access the best offers available and maximising their utility.



At the same time, traders (especially SMEs) can improve their sourcing strategies, access a wider market through platforms and expand to an extent that would be more difficult without an online intermediary. This ability to expand and reach beyond national borders facilitates cross-border e-commerce.

1.3 Transparency of online platforms and reliability of trust mechanisms

Rating systems aimed at creating and fostering trust on platforms are already part of the digital economy. Many online services use consumer-generated ratings systems to provide signals of trust and reliability to users. Consumers are aware that these are systems based on the subjective views of other users. Currently, there is no need for fundamental change in this field, as voluntary market solutions are sufficient to address these concerns. An example of good practice in this field is the work of the multi-stakeholders' group on comparison tools. This group developed two sets of compliance criteria together with the EU Commission. The first part seeks to ensure the compliance of comparison tools with the relevant legislation (e.g. Unfair Commercial Practices Directive) and the second part includes principles to further improve the user-friendliness and transparency of comparison tools.

1.4 Competition, switching, access to data and portability

In some cases, a platform's value to each individual user grows with the number of other users. This network effect may potentially affect the incentives for switching between platforms, thereby possibly diminishing consumer choice and effective competition. The potentially negative impact on consumers can be reinforced in some cases by lack of interoperability and by gatekeeper applications.

Bundling between operating systems, applications and application stores could, on the one hand, limit consumer choice, while, on the other, it could benefit consumers, for instance by offering mobile devices working right out of the box.

Platforms can also extend into downstream markets with own applications that compete with other providers. Proportionate instruments that effectively ensure consistent standards and fair competition should be considered wherever necessary.

However, any consideration of issues related to competition, switching, access to data and portability would necessarily have to focus on the specific online platform, the specific data involved, and the specific options available for moving. **Therefore, there does not seem to be an adequate case about why certain business models need special regulation.** It would be difficult to address such issues across all online platforms. As the technical and economic developments cannot be foreseen, it is better to start with a principle and evidence-based approach, rather than a heavy handed, sector specific ex ante regulation. We do not believe that there are systemic problems unique to online platforms that cannot be adequately addressed by the existing legal framework. Given the fast growing and dynamic nature of platforms, an ex-ante, "all-encompassing" and constraining regulation would not be advisable. In order to create a more innovative Europe, with a positive impact on growth and jobs, it is important to avoid creating new rules for every new innovative product or business model. The EU



should support the consideration about competition and antitrust policy as one of the existing instruments sufficiently fit for purpose to address the current challenges. At the same time, it is crucial to ensure that existing rules are effective, fast enough and properly enforced to meet the new challenges and ensuring level playing field.

We do not believe that, for the time being, specific regulation needs to be devised to address these issues. Policy makers should consider how existing rules that apply to platforms – such as antitrust, data protection or copyright - could provide faster interpretation and guidance against the backdrop of new developments to face new challenges, as a result of the way digital markets operate and to ensure timely intervention where needed. Additionally, given the different types of online platforms and their respective business models, the starting point for any analysis of problems that could occur in any online platform should be to conduct a thorough and economically-grounded assessment of the complex and multi-sided platform ecosystem that is relevant to the specific online platform. The focus should therefore be placed on detecting long lasting bottlenecks and implementing appropriate solutions.

Specifically, given the amount of different business models which may fall into the platform category, creating a one-size-fits-all approach to data portability might be detrimental to the digital economy. Portability is a way to address lock-in effects and switching barriers. It should refer only to the relevant asset (data, content, identifier or any other feature) preventing customers from switching. It must also be taken into account that portability requirements that might seem justified in certain B2C business models can threaten intellectual property and endanger trade secrets of companies which operate in a B2B or any other more complex value-chain environments. General obligations on data portability would imply the need to address the issue of data which also contain relevant information on other data subjects. Moreover, requiring detailed instruments to ensure portability (for instance, with specific details of formatting) risks imposing rigid regulatory standards that hamper the development of new kinds of formatting and data handling. Requiring a company to share the results of its work can deter investment and innovation. Data portability should not extend to requiring firms to share sensitive consumer information with rivals, which could violate the terms of a firm's contractual obligations to its users and raise separate individual privacy concerns.

2. TACKLING ILLEGAL CONTENT ONLINE AND LIABILITY OF ONLINE INTERMEDIARIES

The Internet has revolutionised the way billions of people instantly connect around the world. Through a variety of online platforms and services (e.g. search engines, social networks, video sites, blogging tools, auction services, among many others) often called intermediaries, we are able to create content, find information published by others, buy and sell goods and services. The enormous range of online services has been able to grow due to an overall balanced framework applicable to intermediaries. Along these opportunities, however, internet brings also risks in terms of illegal activities or content.



There are different types of intermediaries of online business and there are different roles they play in the value chain as well as different illegal activities occurring online. Accordingly, different liability rules and different solutions apply. This variety should be taken into account and the current framework needs to provide a level-playing field to all players.

In this context, we see no need to reopen the current framework as set out in the E-Commerce Directive and amend Articles 12 to 15. The E-Commerce Directive has proved to be a flexible instrument over time. Its provisions are clear, flexible, technology-neutral and should remain so. They also strike the right balance between the interests of rightholders, consumers and online intermediaries. In addition, recital 42 of the E-Commerce Directive is sufficiently clear to be interpreted and applied in a homogeneous way. In this sense, we also agree with Recital 46 on its current terms¹.

There is no need to revisit the existing categories of intermediary services. Creating new categories of intermediary services each time a new product, activity of service is created is not only unnecessary, it would also render the legislation complex and obsolete.

Requiring online services to monitor every piece of content or imposing harsh liability on them, would negatively impact innovation, free expression, and privacy. It could also add undue costs, red tape and legal uncertainty. In addition, if a service were automatically liable for illegal content, it would be much more likely to remove all sorts of legal content, not only controversial (though legitimate), for fear of facing legal penalties and could risk hampering legal investigations. In the global digital marketplace, it would be a fundamental problem for internet commerce if companies could be subject to a more severe liability regime in Europe, and in particular a burden on European start-ups that could not compete on the same basis as their competitors.

While market – based solutions and self-regulatory models are preferred, consideration of a proposed “duty of care” principle should not impose direct liability on online platforms. Such a principle could not go beyond voluntary measures e.g. systems for notice and action or other mechanisms aimed at effectively and expeditiously fighting against illegal content, or content that violates terms and conditions of service. The adoption of such measures should not be used as the basis for denying the application of the provisions set out in the E-commerce Directive.

It is important to note that online platforms and other internet players should not be blamed per se for the development of online counterfeiting. One should not be mistaken: the problem is counterfeiting not online platforms. However, given the exponential proliferation of counterfeiting in the digital sphere, rightholders can no

¹ *“In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States’ possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.”*



longer be alone in the fight against counterfeiting. Closer cooperation between IP owners, intermediaries, advertisers and payment processors is key to cut the financial resources away from illegal traders.

A cooperative effort should be carried out by all stakeholders, aimed at finding sound, balanced and sustainable solutions for the benefits of all. Making possible a wider availability of legal content online should be part of this effort.

3. DATA AND CLOUD COMPUTING

3.1 Free flow of data and data localisation restrictions

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 general restrictions on the location of data, thus limiting the possibility of data flowing across borders without objective reasons, would undermine the ability of companies to define their business models and therefore be detrimental to competitiveness and growth of EU companies. On the other hand, such transfers must be carried out in accordance with applicable data protection rules, 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 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 in Europe and globally. Such requirements are not only unjustified but also make 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 lack sufficient capacity, upgraded hardware, or experienced security personnel to counter intrusions and detect signals associated with potential breaches. 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.

3.2 Data access and transfer

Big Data and related activities will pave the way for new 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. Big Data is closely linked to the development of Internet-of-things (IoT) activities such as the ability to aggregate data; to process it; to make it accessible through cloud computing; and, to allow interaction in both a B2B and B2C context. In this regard, there is a need for more common standards for data interoperability across sectors such as in energy, health, automotive and finance.

To take advantage of the potential of data-driven economy, legislation and/or guidelines on data protection, data ownership and data security should make the distinction between personal and non-personal data. They must provide clear incentives for pseudonymisation, which is not just one of the possible tools to improve data security, but also a means to significantly decrease the risks for data subjects. A consistent approach to anonymisation and pseudonymisation can offer robust solutions for smart and big data applications.

It is also key to carefully assess and define a balanced approach to the access to data for third parties, and particularly to 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, in particular 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.

We consider that the EU legislation is well equipped to grant sufficient and fair access to and use of data, and safeguarding fundamental interests of data subjects. 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. The data protection relationship between the parties is governed by the Data Protection Directive and related instruments (and will be covered in the future by the General Data Protection Regulation).

3.3 Liability

The issue of liability needs to be generally addressed in contracts between parties and when liabilities are defined in legislation (e.g. the General Data Protection Regulation), there needs to be clarity in roles and responsibilities of the parties. For instance, the future General Data Protection Regulation must refrain from creating a system of joint and several liabilities which, amongst others, would hamper the development of cloud in Europe. In the B2B context, cloud service providers process personal data according to customer instructions. It is the customers' responsibility to determine the lawfulness of such instructions (e.g. to obtain appropriate consent before proceeding with an email marketing campaign) whilst it is the provider's responsibility to deliver the contracted services securely (i.e. to apply appropriate controls in order to achieve availability, integrity, and confidentiality objectives).



3.4 Cloud computing

Cloud is a more and more important application in the data-driven economy. It delivers not only savings to companies related to their IT systems, but it also responds to a specific strategic vision (for instance, allowing the coexistence of different IT systems after an acquisition).

Promoting the use of cloud in Europe is key. Some specific elements must be taken into account:

➤ ***Defining and balancing responsibilities***

In terms of data protection, cloud users/operators are "data controllers", responsible for any data breach and for compliance with data protection regulations. The cloud user makes sure through the contract that appropriate security measures are put in place by the cloud service provider. It is important for legal clarity that there is a clear distinction between the responsibilities of the data controller and data processor. There is already a provision in the current legal framework, in the EU model clauses for the data subject to pursue the processor in cases of negligence.

The Directive on Unfair Terms in consumer contracts ensures that consumers are more than sufficiently protected against unfair terms. It introduces a notion of "good faith" thereby preventing significant imbalances in the rights and obligations of consumers versus those of sellers and suppliers. Terms that are found unfair under the Directive are not binding for consumers. The Directive also ensures that contract terms are drafted in plain and intelligible language and states that ambiguities will be interpreted in favour of consumers. EU countries have implemented effective means under national law to enforce these rights and made sure that unfair terms are no longer used by businesses. In addition the Data Protection Directive reduces technical risks for consumers as it obliges providers of cloud services that they implement appropriate technical and organizational measures to protect consumers' personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Cloud service providers are already under the security requirements of the Data Protection Directive and will be under similar requirements by the new Data Protection Regulation. In light of current practices, during the pre-contractual phase customers are empowered to evaluate the security measures deployed by cloud service providers in order to determine whether they are appropriate and proportionate to their data. Due to economies of scale, cloud service providers are able to develop security capabilities to a level which is very difficult to match.

➤ ***Transparency on applicable rules and requirements***

In order to reinforce security and trust in the cloud, which is a pre-condition for cloud uptake, transparency could be achieved by setting up a voluntary checklist of cloud contracts possible requirements:



- list the countries where data is likely to be located, including those from which data access can occur (e.g. in case of remote maintenance);
- list of cloud supplier’s subcontractors;
- provider's contractual obligations (safety, responsibility, confidentiality, reversibility, data protection).

➤ **Promoting cloud certification**

Voluntary European level certification, based on international standards, can be very useful in ensuring state-of-the-art level security measures and compliance with the current law.

➤ **Promoting interoperability**

Cloud interoperability is important to ensure a competitive market and avoid lock-in. As public and private organisations move to cloud computing, users should not overlook the implications of switching vendors in the future. For example, open interfaces and data formats—based on open standards - are important to ensure users retain the ability to efficiently transfer their data in the future.

Closed or proprietary interfaces may cede key decisions and options to the discretion of the cloud provider. Closed interfaces and data formats may also limit the ability of the user to efficiently transfer their data in the future. Users need to look well ahead and anticipate that they may wish to move part or all of their data to another cloud environment or they may want to move certain implementations into or out of the cloud that they are seeking to use or build.

4. COLLABORATIVE ECONOMY

The collaborative economy offers new opportunities for innovative business models, and is, on the other hand, a big challenge to traditional businesses. The approach to the collaborative economy must take into consideration that same rules and duties must apply in same economic activities.

Furthermore, this key principle must be the framework in which collaborative economy should be analysed.

4.1 Implications of the development of the collaborative economy

The Commission defines the sharing economy, as *linking individuals and/or legal persons through online platforms (collaborative economy platforms) allowing them to provide services and/or exchange assets, resources, time, skills, or capital, sometimes for a temporary period and without transferring ownership rights.*



As a general consideration, BUSINESSEUROPE firmly believes that the collaborative economy could offer new opportunities for innovative business models. Some studies² estimate that five key sharing sectors – travel, car-sharing, finance, staffing and entertainment – may have the potential to increase global revenues from \$15 billion today to around \$335 billion by 2025.

These new forms of offer and consumption can enable a different use of resources, such as private assets considered underused by their owners. **The collaborative economy enables operators to offer services in an innovative way.**

The collaborative economy can also foster entrepreneurship through the establishment of partnerships between big corporations and start-ups. Some of them have already been established (e.g. Marriott/LiquidSpace or Google/Lending club). Moreover, the collaborative economy allows citizens to provide services themselves – making them entrepreneurs – through the assets they consider under used, which are at the basis of the development of this kind of activities.

These developments can lead to the adoption of **flexible forms of employment** (especially women, young people or people outside the classic job market) that would not exist otherwise.

The collaborative economy can also prompt competition in traditional markets, delivering general increased consumers' welfare, but it is important to bear in mind that competition between collaborative economy and traditional markets must be fair.

At the same time, these new business models can undermine the level playing field between new and tradition business models providing similar services under a different regulatory framework. These developments should be carefully monitored in order to assess where regulation of existing business models is still up to date and necessary to fulfil public aims or whether a more general approach should be taken by assessing the need to update existing regulatory regimes as well.

This is particularly relevant in the context of the application of taxes, requirements to be accomplished related to safety and health measures or **social security and employment rules**. These require a consistent European approach.

For instance, it may in some cases be unclear whether people working through sharing economy platforms should be considered employees of that platform or self-employed. There is no “one-size-fits-all” solution, and Member States have their own respective criteria to differentiate between employees and self-employment. These criteria can also be used in the context of the collaborative economy. In this context, we encourage the European Commission to carry out an adequate impact assessment regarding the need for regulatory action while encouraging Member States to ensure fair competition.

Another issue that is being discussed is the access of freelancers to social safety nets. Without prejudice and respecting how Member States have found different solutions for

² PriceWaterhouseCoopers, The sharing economy – sizing the revenue opportunity, <http://www.pwc.co.uk/issues/megatrends/collisions/sharingeconomy/the-sharing-economy-sizing-the-revenue-opportunity.html>



the social security of self-employed people, it is important to ensure freelancers have good access to benefits such as pensions, unemployment, sickness or disability insurance.

It may also be worth reflecting on how sharing economy companies should deal with people working through them. For example, if a platform deactivates a person's account for a reason that a person believes unfair, and consequently he or she loses their whole business. Also, when people working under an online collaborative economy model build up their online reputation through comments and ratings by users, the question arises about who owns that reputation and whether it should be possible for workers to keep it, even if they decide to change the collaborative platform they are working through.

Finally the collaborative economy challenges traditional ways of consumption and, generally, the usual consumers' habits. It was born as a marginal phenomenon, targeting specific categories of users. Its development may create uncertain systems of liabilities, insurance and health and safety measures related to the shared assets, making both providers and consumers unclear about their rights and obligations. This should be assessed thoroughly.

4.2 Adopting a careful approach to the collaborative economy

Given the recent development of collaborative economy business model, and the absence of a clear picture of the state of play in Europe, we recommend adopting an extremely careful approach to avoid stifling the huge potential for innovation in this area and assess how best to deal with the aspects raised above.

The EU role is particularly important to avoid divergent approaches at national level, which are already creating fragmentation within the Single Market. In order to achieve a level-playing field and allow companies to scale-up, innovate and bring growth to the EU digital economy, it is essential to minimise divergent national (and local) regulatory approaches. At the same time, national practices and legislation which are currently well functioning and established in Member States should not be undermined.

Fostering trust is necessary – not only in the value exchanged, but also in the platform which makes the interaction possible and in the other networks participants. This can be done through awareness raising, strengthening peer review and comparison tools mechanisms (for instance, through trustmarks), or making sure that existing legislation is fit for purpose. For instance, the future EU Data Protection Regulation must avoid creating disproportionate burdens for companies in collecting and using personal data, which are essential for the development of collaborative economy. At the same time, such regulation needs to adequately protect EU citizens' privacy, allowing them to actively participate to the development of these business models – for instance, leaving to company the possibility to achieve data protection objectives using the means they would consider the most appropriate.

As it stands for traditional businesses, access to finance must be facilitated for entrepreneurs and start-ups in the collaborative economy area, also outside the “regular channels” (e.g. through crowdfunding or peer-to-peer lending). In addition, it would be useful to foster public funding in favour of the collaborative economy,



particularly when it benefits cities or local entities (e.g. when the asset is public buildings that can be used as shared working space).
