Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy (EN)

Bitkom's General Remarks on the consultation

General Information

Bitkom welcomes the opportunity to contribute to the public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, as we believe that these issues deserve in-depth consultation with all parties involved and analysis before rushing into any legislative action.

However, we would like to outline the difficulties we encountered in trying to respond to the questionnaire built by the European Commission. We regret, for instance, that sections for comments were not made available for every question of the consultation as such availability depended on the answer given – yes or no. This constitutes a missed opportunity for respondents to explain their position as well as for the European Commission to understand the context and the reasons why a specific position is taken. We also regret the phrasing of many questions, for which we see a degree of bias that will result in misleading answers from the respondents. Finally, the questionnaire lists a selection of assumed practices of platforms – Section IV of the first of part of the consultation - out of context and in isolation from each other.

This version slightly differs from the version we have submitted to the Commission. It shows the answers Bitkom would have given without the problems mentioned above.

Objectives and General Information

General Information

The views expressed in this public consultation document may not be interpreted as stating an official position of the European Commission. All definitions provided in this document are strictly for the purposes of this public consultation and are without prejudice to differing definitions the Commission may use under current or future EU law, including any revision of the definitions by the Commission concerning the same subject matters.

You are invited to read the privacy statement attached to this consultation for information on how your personal data and contribution will be dealt with.

Please complete this section of the public consultation before moving to other sections

- Respondents living with disabilities can request the questionnaire in .docx format and send their replies in email to the following address: CNECT-PLATFORMS-CONSULTATION@ec.europa.eu.
- If you are an association representing several other organisations and intend to gather the views of your members by circulating the questionnaire to them, please send us a request in email and we will send you the questionnaire in .docx format. However, we ask you to introduce the aggregated answers into EU Survey. In such cases we will not consider answers submitted in other channels than EU Survey.
- If you want to submit position papers or other information in addition to the information you share with the Commission in EU Survey, please send them to

CNECT-PLATFORMS-CONSULTATION@ec.europa.eu and make reference to the "Case Id" displayed after you have concluded the online questionnaire. This helps the Commission to properly identify your contribution.

- Given the volume of this consultation, you may wish to download a PDF version before responding to the survey online. The PDF version includes all possible questions. When you fill the survey in online, you will not see all of the questions; only those applicable to your chosen respondent category and to other choices made when you answer previous questions.

Please indicate your role for the purpose of this consultation

- ○ An individual citizen
- ○ **An association or trade organization representing consumers**
- ○ An association or trade organization representing businesses
- ○ An association or trade organization representing civil society
- ○ An online platform
- ○ A business, including suppliers using an online platform to provide services
- ○ A public authority
- ○ A research institution or Think tank
- ○ Other

Please describe the type of online platforms that you represent, a brief description of the online platform and indicate its name and web address

---

Please briefly explain the nature of your activities, the main services you provide and your relation to the online platform(s) which you use to provide services

Bitkom represents more than 2,300 companies in the digital sector, including 1,500 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. Comprising 1,000 small and medium-sized businesses as well as 300 start-ups and nearly all global players, Bitkom' members offer a wide range of software technologies, IT-services, and telecommunications or internet services. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 78 percent of the companies' headquarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focussing the modernization of the education sector and a future-oriented network policy.

Are you a SME or micro enterprise?

- ○ Yes
- ◉ **No**

Please specify

Please indicate your country of residence

- Austria
- Belgium
- Bulgaria
- Czech Republic
- Croatia
- Cyprus
- **Germany**
- Denmark
- Estonia
- Greece
- Spain
- Finland
- France
- Hungary
- Ireland
- Italy
- Lithuania
- Luxembourg
- Latvia
- Malta
- The Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Sweden
- United Kingdom
- Non-EU country

Please specify the Non-EU country

Please provide your contact information (name, address and e-mail address)

Name: Marie-Teresa Weber, Bitkom e.V.

Address: Albrechtstrasse 10, 10117 Berlin

E-mail: mt.weber@bitkom.org

Is your organisation registered in the Transparency Register of the European Commission and the European Parliament?

Note: If you are not answering this questionnaire as an individual, please register in the Transparency Register. If your organisation/institution responds without being registered, the Commission will consider its input as that of an individual and will publish it as such.

- **Yes**
- No
- Non-applicable

Please indicate your organisation's registration number in the Transparency Register

5351830264-31

If you are an economic operator, please enter the NACE code, which best describes the economic activity you conduct. You can find here the NACE classification.

The Statistical classification of economic activities in the European Community, abbreviated as NACE, is the classification of economic activities in the European Union (EU).

I object the publication of my personal data

- Yes
- **No**

Please provide a brief justification.

Online platforms

Online Platforms

SOCIAL AND ECONOMIC ROLE OF ONLINE PLATFORMS

Do you agree with the definition of "**Online platform**" as provided below?

"Online platform" *refers to an undertaking operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups. Certain platforms also qualify as Intermediary service providers. Typical examples include general internet search engines (e.g. Google, Bing), specialised search tools (e.g. Google Shopping, Kelkoo, Twenga, Google Local, TripAdvisor, Yelp,), location-based business directories or some maps (e.g. Google or Bing Maps), news aggregators (e.g. Google News), online market places (e.g. Amazon, eBay, Allegro, Booking.com), audio-visual and music platforms (e.g. Deezer, Spotify, Netflix, Canal play, Apple TV), video sharing platforms (e.g. YouTube, Dailymotion), payment systems (e.g. PayPal, Apple Pay), social networks (e.g. Facebook, Linkedin, Twitter, Tuenti), app stores (e.g. Apple App Store, Google Play) or collaborative economy platforms (e.g. AirBnB, Uber, Taskrabbit, Bla-bla car). Internet access providers fall outside the scope of this definition.*

- ○ Yes
- ○ **No**

Please explain how you would change the definition

- We do not see the necessity for an artificially created, overarching definition for the term online platform and an additional layer of EU-wide regulation of services which could fall under that newly created definition.

- Platforms exist online and offline (e.g. rail networks, car platforms, market places). There are more differences than similarities between platforms, whether online or offline. It is therefore no surprise that they are already regulated in very different ways. Regarding the platforms mentioned in the definition there are already extensive means for regulation both on the national and EU level.

- The ongoing process to expand regulation is misleading. Existing obligations for services rather should be reviewed about their evidence or whether they are already adequately established in other existing rules. Remaining sector specific obligations should be applied equally to equivalent services.

What do you consider to be the key advantages of using online platforms?

Online platforms…

- ☐ **make information more accessible**
- ☐ **make communication and interaction easier**
- ☐ **increase choice of products and services**
- ☐ **create more transparent prices and the possibility to compare offers**

- [ ] **increase trust between peers by providing trust mechanisms (i.e. ratings, reviews, etc.)**
- [ ] **lower prices for products and services**
- [ ] **lower the cost of reaching customers for suppliers**
- [ ] **help with matching supply and demand**
- [ ] **create new markets or business opportunities**
- [ ] **help in complying with obligations in cross-border sales**
- [ ] **help to share resources and improve resource-allocation**
- [ ] **others:**

Please specify:

They increase efficiency, innovation, decrease promotion costs, lead to growth, jobs, more consumer choice.

Have you encountered, or are you aware of problems faced by **consumers** or **suppliers** when dealing with online platforms?

__"Consumer"__ is any natural person using an online platform for purposes outside the person's trade, business, craft or profession. __"Supplier"__ is any trader or non-professional individual that uses online platforms to provide services to third parties both under their own brand (name) and under the platform's brand.

- ○ Yes
- ○ **No**
- ○ I don't know

Please list the problems you encountered, or you are aware of, in the order of importance and provide additional explanation where possible.

How could these problems be best addressed?

- ○ market dynamics
- ○ regulatory measures
- ○ self-regulatory measures
- ○ a combination of the above

TRANSPARENCY OF ONLINE PLATFORMS

Do you think that online platforms should ensure, as regards their own activities and those of the **traders** that use them, more transparency in relation to:

a) information required by consumer law (e.g. the contact details of the supplier, the main characteristics of products, the total price including delivery charges, and consumers' rights, such as the right of withdrawal)?

"Trader" *is any natural or legal person using an online platform for business or professional purposes. Traders are in particular subject to EU consumer law in their relations with consumers.*

- Yes
- **No**
- I don't know

b) information in response to a search query by the user, in particular if the displayed results are sponsored or not?

- Yes
- **No**
- I don't know

c) information on who the actual supplier is, offering products or services on the platform

- Yes
- **No**
- I don't know

d) information to discourage misleading marketing by professional suppliers (traders), including fake reviews?

- Yes
- **No**
- I don't know

e) is there any additional information that, in your opinion, online platforms should be obliged to display?

A fair balance must be struck between different service types by reviewing the existing requirements for traditional service providers, which in some cases are excessively burdensome without delivering added value for consumers, rather than by increasing the requirements for innovative service platforms. Generally, legislation is in place to address all issues above-mentioned, for example in form of the CRD or the UCPD which includes provisions regarding information requirements for consumers.

Have you experienced that information displayed by the platform (e.g. advertising) has been adapted to the interest or recognisable characteristics of the user?

- **Yes**
- No
- I don't know

Do you find the information provided by online platforms on their terms of use sufficient and easy-to-understand?

- **Yes**
- No

What type of additional information and in what format would you find useful? Please briefly explain your response and share any best practice you are aware of. (1500 characters maximum)

Do you find reputation systems (e.g. ratings, reviews, certifications, trustmarks) and other trust mechanisms operated by online platforms are generally reliable?

- **Yes**
- No
- I don't know

Please explain how the transparency of reputation systems and other trust mechanisms could be improved?

What are the main benefits and drawbacks of reputation systems and other trust mechanisms operated by online platforms? Please describe their main benefits and drawbacks.

Reputation systems and trust mechanisms are a functioning, wide-spread market practice, effectively signalling trust and reliability to users, and need not be changed. Reputation is a key driver for companies to take action improving their product/service based on such reviews. The EC shall differentiate trustmarks, certificates and user-generated ratings. Trustmarks assure users upfront that a seller is validated. User-generated review types help consumers to make informed decisions by providing orientation and transparency. Consumers are fully aware that these are based on subjective views. Hence they foster user sovereignty. Reputation systems give online communities an important role improving the online marketplace. They can boost competition between businesses on their products' reliability, on service quality and even facilitate market entry or expansion. 'House rules" often go beyond legal requirements, striking a balance between enabling free expression and a responsible, safe environment. Enforcement tools allow users to flag content so that

intermediaries can directly react to any breaches of the rules.

The implementation of the UCP 2005/29/EC[1] will improve transparency and complementary industry best practices provide relevant consumer information. We don't consider an added state-run reputation portal necessary or useful.

USE OF INFORMATION BY ONLINE PLATFORMS

In your view, do online platforms provide sufficient and accessible information with regard to:

a) the personal and non-personal data they collect?

- **Yes**
- No
- I don't know

b) what use is made of the personal and non-personal data collected, including trading of the data to other platforms and actors in the Internet economy?

- **Yes**
- No
- I don't know

c) adapting prices, for instance dynamic pricing and conditions in function of data gathered on the buyer (both consumer and trader)?

- **Yes**
- No
- I don't know

Please explain your choice and share any best practices that you are aware of.

Existing legislation has allowed widespread best practices to develop across the industry. For instance, Directive 95/46/EC contains obligations to inform data subjects (including users of online platforms) about the collection of personal data, including the fact that personal data is being collected, the identity of the controller and the purpose of the processing. These obligations will become even more detailed in the upcoming General Data Protection Regulation (see in particular Chapter III of legal text). These information provision requirements encompass a very broad range of data, practically anything that has the potential of identifying an individual. Given the very detailed existing and upcoming legislation in this field, additional service specific requirements do not seem necessary.

---

[1] The UK Competition Markets Authority recommendations or similar efforts at EU level clarify the legal framework for online review tools.

Please share your general comments or ideas regarding the use of information by online platforms

Collecting and analysing data is becoming an inherent part of commercial activity. Understanding data can help businesses create better products and services and work more efficiently. None of these benefits are unique to digital businesses or Internet services.

Platforms must ensure that they provide a high level of security for the information they handle as in the highly competitive landscape, the trust of users and their general eco-system is often a market differentiator. At the same time Platforms must be able to provide an added value for its users. This requires finding a balance between allowing room for different business models to exist, whilst ensuring the highest level of privacy rights.

Data privacy and protection of user information is demanded by users and is a very important priority for many online businesses. Users care about privacy and companies must address this concern in order to keep users from jumping to alternative options.

As “platforms” include various business models and they vary in their collection and use of data, it is not possible to specify the role of data in platform businesses. Data-related questions should be considered separately to the discussion on platforms.

Rather than adding a new layer of information requirements for platforms, the existing information requirements within horizontal consumer legislation should be reviewed as part of the REFIT exercise ensuring consumer protection irrespective of the business model.

In the spirit of a level playing field, an approach of deregulation should be adopted which limits hard-regulation to a level of principles and leaves room for implementing issues and details to more flexible instruments of self- and co-regulation such as those recommended in the Better Regulation Toolbox of the EU-Commission for areas of fast technological change.

RELATIONS BETWEEN PLATFORMS AND SUPPLIERS/TRADERS/APPLICATION DEVELOPERS OR HOLDERS OF RIGHTS IN DIGITAL CONTENT

Please provide the list of online platforms with which you are in regular business relations and indicate to what extent your business depends on them (on a scale of 0 to 3). Please describe the position of your business or the business you represent and provide recent examples from your business experience.

	Name of online platform	**Dependency** (0: not dependent, 1: dependent, 2: highly dependent)	**Examples from your business experience**
1			
2			
3			
4			
5			

How often do you experience the following business practices in your business relations with platforms?

The online platform …

** A parity clause is a provision in the terms of use of an online platform or in an individual contract between the online platform and a supplier under which the price, availability and other conditions of a product or service offered by the supplier on the online platform have to maintain parity with the best offer of the supplier on other sales channels.*

	Never	**Sometimes**	**Often**	**Always**
requests me to use exclusively its services				
applies “parity clauses" *				
applies non-transparent fees				
applies fees without corresponding counter-performance				
applies terms and conditions, which I find unbalanced and do not have the possibility to negotiate				
unilaterally modifies the contractual terms without giving you proper notification or allowing you to terminate the contract				
limits access to data or provides it in a non-usable format				
puts significant constraints to presenting your offer				
presents suppliers/services in a biased way				
refuses access to its services unless specific restrictions are accepted				
promotes its own services to the disadvantage of services provided by suppliers				

If you do experience them, what is their impact on your business activity (on a scale from 0 to 3).

Impact on my business:

The online platform …

** A parity clause is a provision in the terms of use of an online platform or in an individual contract between the online platform and a supplier under which the price, availability and other conditions of a product or service offered by the supplier on the online platform have to maintain parity with the best offer of the supplier on other sales channels.*

	0 – no impact	**1 – minor impact**	**2 – considerable impact**	**3 – heavy impact**
requests me to use exclusively its services				
applies “parity clauses" *				
applies non-transparent fees				
applies fees without corresponding counter-performance				
applies terms and conditions, which I find				

unbalanced and do not have the possibility to negotiate				
unilaterally modifies the contractual terms without giving you proper notification or allowing you to terminate the contract				
limits access to data or provides it in a non-usable format				
puts significant constraints to presenting your offer				
presents suppliers/services in a biased way				
refuses access to its services unless specific restrictions are accepted				
promotes its own services to the disadvantage of services provided by suppliers				

If you are aware of other contractual clauses or experience other potentially problematic practices, please mention them here

No.

Please briefly describe the situation

The platform and app economy leads to jobs and to growth. It thus has a positive impact on the European economy. Today over 50% of people in a number of countries in Europe have a smartphone and there are over one million apps available from apps stores.[2] The proliferation of apps is also the underlying driver of investment in ubiquitous broadband wireless networks including public Wi-Fi and 4G. These investments would not have happened in the absence of apps, as apps are driving consumer demand and willingness to pay for enhanced wireless access.[3] Europe has a vibrant app producing sector which generates significant revenues and jobs.[4] The sector continues to grow, driven by global smart device adoption and European excellence in specific verticals including, for example, music and financial services.[5] European developer revenues account for an estimated 35% 12 of global app revenues, a substantial share in comparison with the overall share of global technology company revenues attributed to Europe. Figure 2-2 shows total annual app revenues generated by European app developers (70% of which are paid out to developers).[6] A significant number of jobs are also attributed to app development and associated activity, but available estimates differ.[7] A study for the European Commission estimated that there were 1.8 million direct apps jobs of which 1 million technical jobs in February 2014[8] whilst Vision Mobile estimated that there were 846,000 direct technical jobs

[2] http://www.plumconsulting.co.uk/pdfs/Plum_March_2015_All_about_that_app.pdf, S.4.
[3] http://www.plumconsulting.co.uk/pdfs/Plum_March_2015_All_about_that_app.pdf, S.8, WSJ. November 2014. "European Telecoms Bet on Data, Investment in 4G Infrastructure." http://online.wsj.com/articles/european-telecoms-bet-on-data-investment-in-4g-infrastructure-1416571267.
[4] http://www.plumconsulting.co.uk/pdfs/Plum_March_2015_All_about_that_app.pdf, S.11.
[5] http://www.plumconsulting.co.uk/pdfs/Plum_March_2015_All_about_that_app.pdf, S.11.
[6] http://www.plumconsulting.co.uk/pdfs/Plum_March_2015_All_about_that_app.pdf, S.12, 13 Estimated from reported global revenue figures from Apple and Google, scaled down to Europe by the ratio of 35%.
[7] http://www.plumconsulting.co.uk/pdfs/Plum_March_2015_All_about_that_app.pdf, S. 12.
[8] Gigaom. February 2014. "Sizing the EU App Economy." http://eurapp.eu/sites/default/files/Sizing%20the%20EU%20App%20Economy.pdf.

and 456,000 direct non-technical jobs in 2015 (approximately double a previous estimate by Vision Mobile).[9]

Are you a holder of rights in digital content protected by copyright, which is used on an online platform?

- **Yes**
- No

As a holder of rights in digital content protected by copyright have you faced any of the following circumstances:

An online platform such as a video sharing website or an online content aggregator uses my protected works online without having asked for my authorisation.

- **Yes**
- No

An online platform such as a video sharing website or a content aggregator refuses to enter into or negotiate licensing agreements with me.

- Yes
- No

An online platform such as a video sharing website or a content aggregator is willing to enter into a licensing agreement on terms that I consider unfair.

- Yes
- No

An online platform uses my protected works but claims it is a hosting provider under Article 14 of the E-Commerce Directive in order to refuse to negotiate a licence or to do so under their own terms.

- Yes
- No

As you answered YES to some of the above questions, please explain your situation in more detail.

A multitude of providers, namely host providers, do not use creative works themselves. The online services listed in the proposed definition of platforms are diverse in nature, ranging from online content stores to e-commerce websites. They may allow users to sell second-hand DVDs, enable the online distribution of films, music or books, host videos online or allow users to share photos. Depending on the situation, the acquisition of a license, the granting of a permission, the application of an exception or any application of the E-

[9] Vision Mobile. February 2015. "European App Economy 2015". https://www.developereconomics.com/reports/european-app-economy-2015/.

commerce liability rules may play a role. Finally, most services listed in the questions above are considered information society services coming under the scope of the E-commerce Directive. The current system succeeds in striking a good balance for all parties. In a larger context and outside of the presently-discussed regulatory system, Bitkom sees room for improvement by means of efficient concerted industry initiatives to fight content piracy at its roots and therefore endorses the Follow the Money approach on a pan-European level to dry out piracy. Furthermore a better and more widespread availability of legal offers that are attractive to consumers will improve the situation for the creative and cultural sectors as well as adjacent information and communication sectors.[10]

Is there a room for improvement in the relation between platforms and suppliers using the services of platforms?

- No, the present situation is satisfactory.
- Yes, through market dynamics.
- **Yes, through self-regulatory measures (codes of conducts / promotion of best practices).**
- Yes, through regulatory measures.
- Yes, through the combination of the above.

Are you aware of any dispute resolution mechanisms operated by online platforms, or independent third parties on the business-to-business level mediating between platforms and their suppliers?

- **Yes**
- No

Please share your experiences on the key elements of a well-functioning dispute resolution mechanism on platforms

One good example for a well-functioning mechanism is the Uniform Domain-Name Dispute-Resolution Policy (UDRP), a process established by ICANN for the resolution of disputes on registration of internet domain names. It is the oldest online dispute resolution system and has proven itself ever since. UDRP has decided on 35,000+ of such cases. Overall, it has shortened proceedings duration, eased enforcement and has a global reach. Its success can be attributed to the highly-skilled professionals it employs.

There are examples of well-functioning dispute resolution mechanisms on a voluntary basis in compliance with the eCD's principles. Additional regulation should be avoided which would adversely affect the sensible balance of all interests concerned in the distribution of and access to information on the Internet. Some traditional business models may still need time to adapt fully to the digital economy, and the EU legislator should not interfere with this process. It should be secured that consumer choice as well as media pluralism are maintained, that freedom of information and expression are not hampered, that no harm is done to innovation/investment. Therefore, Bitkom considers inadequate and ineffective to

[10] European Commission, Joint Research Centre, Institute for Prospective Technological Studies: Streaming Reaches Flood Stage: Does Spotify Stimulate or Depress Music Sales? Available under: https://ec.europa.eu/jrc/sites/default/files/JRC96951.pdf.

ponder upon inappropriate tools such as ancillary rights protection or alike measures, the negative implications of which can already be seen.[11]

Regarding consumer alternative dispute resolution, the horizontal rules of the ADR (dir. 2013/11/EU) are applicable.

CONSTRAINTS ON THE ABILITY OF CONSUMERS AND TRADERS TO MOVE FROM ONE PLATFORM TO ANOTHER

Do you see a need to strengthen the technical capacity of online platforms and address possible other constraints on switching freely and easily from one platform to another and move user data (e.g. emails, messages, search and order history, or customer reviews)?

Yes

No

If you can, please provide the description of some best practices (max. 5)

	Name of the online platform	**Description of the best practice** (max. 1500 characters)
1.		
2.		
3.		
4.		
5.		

Should there be a mandatory requirement allowing non-personal data to be easily extracted and moved between comparable online services?

Yes

No

Please explain your choice and share any best practices that you are aware of. (1500 characters maximum)

Please share your general comments or ideas regarding the ability of consumers and traders to move from one platform to another

We observe and welcome that online traders/consumers are always freely able to move between platforms. This is the essence of consumer choice online, and also holds for ECS. Many online services offer best in class portability to users and many traders offer their products and services on competing online platforms to their own advantage. Online platforms and ECS are therefore incentivised by business reasons to make efforts to ensure

[11] Dissenting opinion: Bertelsmann SE & Co. KGaA does not support the Bitkom position regarding ancillary rights for press publishers.

compatibility for sellers/traders using various online platforms.

A recent Oxera study found that businesses and consumers in fact easily use multiple services for similar purposes with ease and do not report 'lock-in'. Any regulatory initiative would therefore be disproportionate as long as services do not foster lock-in effects which create a significant obstacle to user switching.

So while we support portability principles we caution against strict legal requirements: Requiring specific formatting details risks replacing innovation in proprietary standards with consistent but inflexible government-mandated standards that deter the development of new kinds of formatting and data handling. Requiring firms to share the fruits of their labour deters investment, innovation, and economic growth. Requiring firms to share sensitive consumer information could violate the terms of a firm's contractual obligations to its users and raise separate individual privacy concerns. Requiring controllers to transfer personal data may cause disproportionate cost and effort (particularly in markets without lock-in effects) and may compromise valuable proprietary information and intellectual property.

Hence any data portability provisions must reflect technological reality, respect technological neutrality and allow for the continued development of dynamic digital businesses. They mustn't impose requirements virtually impossible for companies to fulfil nor unnecessary administrative burden. Regulatory intervention does not appear necessary as the market provides adequate data portability solutions to users.

A best practice example for support principles around interoperability and portability of data to promote user choice and switching is Google Takeout. This service allows users to download their data (emails, calendar, information, contacts, etc.) and move them easily across to another service, thus encouraging choice and competition.

Portability of personal data is furthermore addressed in the draft General Data Protection Regulation which enables individuals to transfer data between service providers. Data portability is relevant for privacy (individual control over personal data) but also for competition law (reducing lock-in effects). Depending on the circumstances, data portability restrictions may qualify as abuse of dominance (Art.102 TFEU).

ACCESS TO DATA

As a trader or a consumer using the services of online platforms did you experience any of the following problems related to the access of data?

a) unexpectedly changing conditions of accessing the services of the platforms

Yes

No

b) unexpectedly changing conditions of accessing the Application Programming Interface of the platform

Yes

No

c) unexpectedly changing conditions of accessing the data you shared with or stored on the platform

Yes

No

d) discriminatory treatment in accessing data on the platform

Yes

No

Would a rating scheme, issued by an independent agency on certain aspects of the platforms' activities, improve the situation?

Yes

No

Please explain your answer

It is unclear what type of rating system the EC has in mind and for which platforms. It would be difficult and highly complex to define a uniform set of criteria that could apply to all platforms and will take into account the diversity of business models. Furthermore, creating a rating system for the online world would further increase the imbalance with the offline world, where no such rating system is available. The objective of the DSM should be to narrow the gap between the off- and the online world. Therefore rating schemes should be voluntary and their design should be left to the market players.

While it is important to understand that changes to access to data may represent inconveniences to consumers, it is important for business to retain the possibility to adjust their services and the related terms of use to the changing business environment. This is in particular true in the online environment, which is clearly characterised by dynamic and constant change. While businesses already make important efforts to highlight the changes they make, any obligation that would prohibit companies to adjust their business practices to the competitive environment and even more importantly to the ever evolving needs of their customers would be hugely detrimental to European businesses. Such new rules would hit start-ups especially hard as they would lose their nimbleness, one of their key advantages they hold over bigger competitors.

Please share your general comments or ideas regarding access to data on online platforms

Trust and security in digital services is a key factor to the Digital Single Market. EU data protection rules must find a balance to ensure that they meet the expectations of consumers while being fit for purpose for businesses. However, the current approach taken to update the EU data protection framework for the digital age risks undermining the aspirations and vision of the DSM strategy. By creating greater legal uncertainty and more red tape across the Member States, as well as potentially establishing incentives for gathering more data than required, this could potentially hinder the development of the DSM and European businesses and damage privacy and consumer confidence online.

The high level of innovation activity on digital markets is favoured by low barriers to market entry and access to data. Data in the digital age is akin to sunshine, it is a renewable resource that many actors can use to build a successful business. Digitalisation and the

Internet in particular, have reduced a whole range of economic costs for businesses. As the German Monopolies Commission has highlighted in their recent special report on “The challenge of digital markets”: “Through such cost reduction companies can set up and expand their operations very quickly. In addition, whereas high investment costs can frequently make a market entry difficult, such costs have in recent times increasingly become variable costs in certain parts of the digital economy. This is the case where computing power or storage space can be rented by companies to fit their needs, for instance thanks to new technologies (e.g. cloud computing) or open source software. These lower barriers to entry increase competition in digital markets.

The following ideas are to be understood in a wider sense. They are not only valid for the question of access to data on online platforms but are meant to describe the question of new regulation of “platforms” as described in this first part of the consultation questionnaire.

Regulators should keep in mind that any intervention should be closely targeted to the specific harm identified on the facts. With a view to secure a level playing field among services, regulators should focus on the question if these services exercise similar or equivalent functions and if there is evidence based on facts for a specific harm caused by these services. If this is the case, similar rules should be applied to similar services, with every care given to avoid disproportionate actions and unwelcome side-effects that could hamper innovation in what is a very dynamic and rapidly evolving space. The answer is simplification; not additional layers of regulatory complexity. If there is no evidence based on facts for a specific harm caused by services which are currently already subject to regulation, there should also be room for deregulation.

Tackling illegal content online and the liability of online intermediaries

Tackling illegal content online and the liability of online intermediaries

Please indicate your role in the context of this set of questions

*Terms used for the purposes of this consultation: **"Illegal content"** Corresponds to the term "illegal activity or information" used in Article 14 of the E-commerce Directive. The directive does not further specify this term. It may be understood in a wide sense so as to include any infringement of applicable EU or national laws and regulations. This could for instance include defamation, terrorism related content, IPR infringements, child abuse content, consumer rights infringements, or incitement to hatred or violence on the basis of race, origin, religion, gender, sexual orientation, malware, illegal online gambling, selling illegal medicines, selling unsafe products. **"Hosting"** According to Article 14 of the E-commerce Directive, hosting is the “storage of (content) that has been provided by the user of an online service”. It may for instance be storage of websites on servers. It may also include the services offered by online market places, referencing services and social networks. **"Notice"** Any communication to a hosting service provider that gives the latter knowledge of a particular item of illegal content that it transmits or stores and therefore creates an obligation for it to act expeditiously by removing the illegal content or disabling/blocking access to it.. Such an obligation only arises if the notice provides the internet hosting service provider with actual awareness or knowledge of illegal content. **"Notice provider"** Anyone (a natural or legal person) that informs a hosting service provider about illegal content on the internet. It may for instance be an individual citizen, a hotline or a holder of intellectual property rights. In certain cases it may also include public authorities. **"Provider of content"** In the context of a hosting service the content is initially provided by the user of that service. A provider of content is for instance someone who posts a comment on a social network site or uploads a video on a video sharing site.*

- individual user
- content provider
- notice provider
- intermediary
- **none of the above**

Please explain

Have you encountered situations suggesting that the liability regime introduced in Section IV of the E-commerce Directive (art. 12-15) has proven not fit for purpose or has negatively affected market level playing field?

- Yes
- **No**

Please describe the situation.

The liability regime of the eCD has proven itself effective and proportionate. It promotes dynamic, competitive markets since its inception. Intermediaries' contributions to the economy would not be possible at the current level without the liability regime in the eCD.

However, while the intention of the eCD is clear and the principles remain valid, experiences have illustrated inconsistencies arising from poor implementation and interpretation. Deficiencies in enforcement create risks for intermediaries.

- It is not always clear at what point an intermediary acquires "knowledge" of an illegal activity. The current lacuna (not in the eCD, but in national law (c.f. BGH, "Blog-Eintrag") forces intermediaries to make some judgment calls in the light of their legal experience, appetite for legal risk and contractual commitments. Some judgment calls might be relatively fuss-free (e.g. child pornography, also some infringement on copyright material). However, many cases (e.g. in areas of defamation, second-hand goods or reuse of copyright material) can be problematic to evaluate. This legal uncertainty is contrary to eCD's intention.

- Despite the eCD a right holder in Germany is entitled to claim an injunctive relief against intermediaries ("Störerhaftung"). This legal construct undermines eCD's liability provisions, exceeds the requirements of the IPRED (Art. 11) and of the InfoSoc-D (Art. 8 (3)), brings about competitive disadvantages and is contrary to the fully-harmonising eCD-provisions.
  Furthermore, the "kino.to" jurisprudence of the CJEU entails concerns: the liability degree is much over-stretched (Art. 12 eCD). Costs, effort, violation of third party rights are not proportionate with regard to the lack of effectiveness (cf. Art. 3 IPRED).Surveys prove that blocking methods are ineffective and do not prevent infringements; access providers are not "best placed to bring such infringing activities to an end" (Rec. 59 InfoSoc-D). This leads to several key concerns:

  - Conflict of "Störerhaftung" with eCD; clarification is needed that limitation of liability applies to claims for injunction;

- Clarification is needed that Art. 8 (3) InfoSoc-D does not refer to claims raised by right holders against access providers;

- if blocking methods would be politically inevitable, this would require (i) a legal framework for procedures ("sufficient and clear legal basis", Rec. 59 InfoSoc-D, Art. 52 Charter), (ii) inclusion of all stakeholders/those affected by action (cf. CJEU "kino.to"), (iii) provision on cost allocation to rightholders (cf. § 101 GCA), (iv) ISP-protection against claims for compensation ("collateral damages" are imminent in any ISP action);

- those situated next to the source of an infringing content must be addressed first ("subsidiarity").

The existing liability regime – the 3 provider-categories and the horizontal application on different infringements in particular – has to be maintained while clarifying certain aspects of its application.

Do you think that the concept of a "mere technical, automatic and passive nature" of information transmission by information society service providers provided under recital 42 of the ECD is sufficiently clear to be interpreted and applied in a homogeneous way, having in mind the growing involvement in content distribution by some online intermediaries, e.g.: video sharing websites?

Yes

No

I don't know

Please explain your answer.

There is no additional requirement that a hosting service be of a "mere technical, automatic and passive nature". That concept is derived from Recital 42 and applies exclusively to the services of mere conduit and caching.

The concept of "mere technical, automatic and passive" information transmission has proven flexible enough to apply in a variety of cases (media law, intellectual property law, privacy, etc.). The CJEU has clarified in several cases (C-236/08 "Google", C-324/09 "L'Oréal", C-70/10 "Scarlet", C-360/10 "SABAM", C-291/13 "Papasavvas") the concepts used in the eCD and harmonized its construction by national courts.

Video sharing websites do not raise specific issues and should not be treated differently than other hosting service providers. Established video sharing sites, unfortunately not all video sharing sites, remove content when they are given notice. Some have developed specific systems to prevent the uploading of copyright infringing content (for example DailyMotion's signature or YouTube's Content ID). With such systems, rightsholders, who cooperate by bringing reference files to the platforms, do not need to issue copyright notices anymore.

However, such systems are only possible because the flexible and proportionate framework of the eCD sets the incentives and space to engineer them. They are no substitutes to the rule of law, require the collaborations of rightholders, and cannot be extended systematically to other types of services.

Mere conduit/caching/hosting describe the activities that are undertaken by a service provider. However, new business models and services have appeared since the adopting of the E-commerce Directive. For instance, some cloud service providers might also be covered under hosting services e.g. pure data storage. Other cloud-based services, as processing, might fall under a different category or not fit correctly into any of the existing ones. The same can apply to linking services and search engines, where there has been some diverging case-law at national level. Do you think that further categories of intermediary services should be established, besides mere conduit/caching/hosting and/or should the existing categories be clarified?

Yes

No

Please provide examples

The right answer to this question should be NO. However, we like to highlight problems with different jurisdiction stretching the EU Directives.

With all arguments considered, retaining the status quo of the eCD (despite the need for clarification as laid out above) and retaining the existing categories of intermediaries is the best to allow businesses and consumers to benefit from digital economy. The key advantage of the eCD is its technological neutrality to adjust to new developments and technologies. It is resilient and future proofed. Diverging case law is due to national legal specificities that are not compatible with the eCD (e.g. "Störerhaftung" in Germany).

While maintaining the wording of the existing categories the Commission should clarify some inconsistencies on national level:

- cloud storage with no freely distributable "link" should under no circumstances lead to liability; cloud storage comparable to hosting should follow the same principles while taking the specific legal/contractual/technical circumstances into account (e.g. on professional secrets or eAdministration);
  "pure linking" (e.g. for providing a reference to a source (cf. German Federal Supreme Court in "Heise-online"; cf. § 14a EC-Act in Austria) should not be of particular relevance in the present context; "enhanced linking", i.e. establishing a genuine business model, might need a differentiated evaluation;

- the genuine activity of search engines should generally not lead to liability.

On the "notice"

Do you consider that different categories of illegal content require different policy approaches as regards notice-and-action procedures, and in particular different requirements as regards the content of the notice?

Yes

No

Do you think that any of the following categories of illegal content requires a specific approach:

Illegal offer of goods and services (e.g. illegal arms, fake medicines, dangerous products unauthorised gambling services etc.)

- [ ] Illegal promotion of goods and services
- [ ] Content facilitating phishing, pharming or hacking
- [ ] Infringements of intellectual property rights (e.g. copyright and related rights, trademarks)
- [ ] Infringement of consumer protection rules, such as fraudulent or misleading offers
- [ ] Infringement of safety and security requirements
- [ ] Racist and xenophobic speech
- [ ] Homophobic and other kinds of hate speech
- [ ] Child abuse content
- [ ] Terrorism-related content (e.g. content inciting the commitment of terrorist offences and training material)
- [ ] Defamation
- [ ] Other:

Please specify.

Please explain what approach you would see fit for the relevant category.

On the "action"

Should the content providers be given the opportunity to give their views to the hosting service provider on the alleged illegality of the content?

- ○ Yes
- ○ **No**

Please explain your answer

Were the intermediary receives the views of the content provider on the alleged illegality of the content, this could not have any legal effect as the intermediary is not dealing with the content per se.

Intermediaries are not best placed to act as judges in cases where illegality is not obvious and undeniable. In addition, they may not have the resources to act as a mediator, passing third party complaints to a content provider and passing the content provider's reply back to the complainant and so on. It is thus understandable (though regrettable) that some intermediaries might take content down without properly examining the asserted grounds for removal. The greater the pressure that is put upon intermediaries in terms of liability and the requirement to use resources to mediate or judge third party disputes, the greater will be the incentive to remove content without carefully reviewing, or otherwise testing the veracity of the notices received.

Before approaching the intermediary, the complainant should make a reasonable effort, making use of the means and information publicly available, to contact the user, webmaster,

or other content provider responsible for posting the objectionable content to the Internet and ask to have it removed.

Such a requirement would provide effective notice to the person most capable of controlling further dissemination of the challenged content: the person who put it online in the first place.

If you consider that this should only apply for some kinds of illegal content, please indicate which one(s)

Should action taken by hosting service providers remain effective over time ("take down and stay down" principle)?

Yes

No

Please explain

An intermediary should not be subjected to proactive monitoring obligations. As confirmed by recent CJEU decisions (SABAM/Scarlet and SABAM/Netlog), such general monitoring obligations were both inconsistent with the letter of the eCD and with important underlying rights of users, including the rights of freedom of expression and access to information. Despite this, German jurisdiction holds monitoring obligations following a notice being legitimate (and not creating a conflict with Art. 15 eCD). This denies the fact that stay-down obligations often also require steady monitoring action (cf. CJEU-decisions cited above).

In addition, even if an intermediary had the technical capacity to put in place stay down measures, it would have no effect. The content would quickly be available somewhere else (on a site that does not play by EU rules) and users would still be able to access it.

Furthermore there is the risk of stifling innovation and competition because newcomers and SMEs might be/remain unable during some course of time to implement respective mechanisms which will have been requested (initially) with reference to major service providers.

It should be observed that the jurisprudence of national courts may represent a cause for concern: in Germany, the German Federal Supreme Court has established the legal construct of so-called “kerngleiche Verstöße”, i.e. a provider is considered to be liable if he does not take action necessary to prevent the reiteration of infringements which are deemed principally similar. In case of negligent ignoring of a renewed appearance of the same illegal content or a similar content (e.g. under a new designation), high risks exists in the context of an injunction judgement or of a cease-and-desist declaration accompanied by a penalty clause. Given that, already in the first place, there are no (widespread) mechanisms which would assist in identifying a specific content, it is even less deceivable that there will be a case for detecting content that in essence is highly similar to the one that has been the object of an action ordered beforehand. Here, clearly, the boundary of the prohibition to request providers to proactively search for possibly illegal content is reached, if not crossed.

Therefore, the underlying problem often is the national implementation and application formulating obligations to prevent future infringements which do not reflect sufficiently on the realities of putting and distributing “information” on the Internet.

On duties of care for online intermediaries:

Recital 48 of the Ecommerce Directive establishes that "[t]his Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities". Moreover, Article 16 of the same Directive calls on Member States and the Commission to encourage the "drawing up of codes of conduct at Community level by trade, professional and consumer associations or organisations designed to contribute to the proper implementation of Articles 5 to 15". At the same time, however, Article 15 sets out a prohibition to impose "a general obligation to monitor".

(For online intermediaries): Have you put in place voluntary or proactive measures to remove certain categories of illegal content from your system?

Yes

No

Please describe them.

Could you estimate the financial costs to your undertaking of putting in place and running this system?

Could you outline the considerations that have prevented you from putting in place voluntary measures?

Bitkom does not have any voluntary measures in place, but we would like to highlight some concerns regarding such measures:

As is the case under the law, a notice and takedown system designed by the eCD should not itself create liability on the intermediary where none exists. Furthermore, there should be no liability where the intermediary acts in good faith to restrict allegedly illegal content. Voluntary systems for notice and action, flagging systems, manual review systems, and other content monitoring/optimization and moderation systems should not be counted against the intermediary, when considering whether the activities of an intermediary are of a merely technical, automatic and passive nature, or whether the intermediary has knowledge of or control over the data. Otherwise, the intermediary is obviously incentivised to take a hands-off approach.

Furthermore the Commission should take into account that pro-active measures always risk to represent censorship and might produce a high rate of “false positive” incidents of content-matching alerts which might infringe the freedom of communication and information and the secrecy of communication.

To incentivize voluntary measures it would be useful to officially approve industry standards or codes of conduct and to grant subscribers of such standards a waiver from any liability. This way the adoption of voluntary standards would lead to a legal advantage (no liability) rather than risking legal disadvantages.

Do you see a need to impose specific duties of care for certain categories of illegal content?

- Yes
- **No**
- I don't know

Please specify for which categories of content you would establish such an obligation. (1500 characters maximum)

Please specify for which categories of intermediary you would establish such an obligation

---

Please specify what types of actions could be covered by such an obligation

---

Do you see a need for more transparency on the intermediaries' content restriction policies and practices (including the number of notices received as well as their main content and the results of the actions taken following the notices)?

- **Yes**
- No

Should this obligation be limited to those hosting service providers, which receive a sizeable amount of notices per year (e.g. more than 1000)?

- Yes
- **No**

Do you think that online intermediaries should have a specific service to facilitate contact with national authorities for the fastest possible notice and removal of illegal contents that constitute a threat for e.g. public security or fight against terrorism?

- **Yes**
- No

Do you think a minimum size threshold would be appropriate if there was such an obligation?

- Yes
- **No**

Please share your general comments or ideas regarding the liability of online intermediaries and the topics addressed in this section of the questionnaire.

The Internet allows anyone, anywhere to instantly connect with billions of people around the world. Through a variety of online services -- search engines, social networks, video sites, blogging tools, auction services, and many others -- we are able to create content, find information published by one other, communicate, and buy and sell goods and services. Platforms and services that help users interact with another are often called “intermediaries”, and as the Internet evolves, so too do intermediaries. Intermediary liability is the concept of holding an online platform responsible for the illegal or harmful content created by users of those services in cases where the right holder cannot enforce the rights with legal actions against the infringer themselves. Who counts as an “intermediary” often includes access providers, search engines, hosting platforms, email providers, payment processors, social networks and many more. The commonality between these entities is that they enable others to do things on the Internet, they are intermediaries in the sense that they provide services that allow for user A to interact with user B in different ways. Requiring online services to monitor every piece of content or imposing harsh liability on them doesn’t make sense -- it would be bad for innovation, free expression, and privacy. This is analogous to the offline world; telephone companies are not forced to monitor people's calls to make sure they are not doing something illegal, and they are not held legally responsible for callers who plan a crime over their phone lines. Imposing liability on online intermediaries may create undue costs and burdens, but also chill innovation by creating legal uncertainty. In addition, if a service were automatically liable for illegal content, it would be much more likely to remove all sorts of controversial (though legitimate) speech, for fear of facing legal penalties. The intermediary liability regime is a standard that can be found in several legislations (US, CA, JP, AU, etc.). It would be a fundamental problem for internet commerce if companies can 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 companies abroad.

Looking at all European Directives dealing with the liability of online intermediaries we would like to point out that the requirements of Art. 11 of the IPR Enforcement Directive and of Art. 8 (3) of the InfoSoc Directive are not sufficiently coordinated with the scope of release from liability in Articles 12 to 14 of the eCD. This is despite the fact that a clear distinction is being made insofar as intermediaries are not released from the responsibility to stop or to prevent infringements (Art. 12 (3), Art. 13 (2) and Art. 14 (3) of the eCD), so that this obligation remains legally enforceable by right holders as foreseen by Art. 11 of the Enforcement Directive and Art. 8 (3) of the InfoSoc Directive. Recent developments in national legislation underline that there is a clear need to assess compatibility with the eCD whenever attempts are undertaken to change the existing balance of interests; a relevant legislative process in Germany has met with profound and large criticism, also from the European Commission (cf. TRIS 2015/02834).

Furthermore, there is no harmonization with respect to the single requirements of an injunctive relief, the bearing of costs of court procedures and previous legal prosecution, the dimension of reasonableness and the bearing of costs of technical prevention measures and the consequences of an accidental breach of the injunctive duties by the intermediary. Intermediaries in the different member states seem to meet different strictly provisions, with different impact on the competitive position.

Additional points which should be taken into consideration by the Commission:

- indemnity from damage claims;
- provision of procedural safeguards in national legislation in order to meet requirements stipulated by CJEU;

- introduction of a principle of subsidiary action, that is, alleged infringements should be addressed to, and cleared in respect of, the entity which is closest to the source of the action under scrutiny. The “follow-the-money approach” represents a useful attempt to implement the basic idea of this principle; furthermore, in case an Internet access provider cannot for objective reasons contribute to putting an end to an illegal online activity or the illegal publishing of content over the Internet, he cannot become the object of an obligation.

Data and cloud in digital ecosystems

Data and cloud in digital ecosystems

FREE FLOW OF DATA

ON DATA LOCATION RESTRICTIONS

In the context of the free flow of data in the Union, do you in practice take measures to make a clear distinction between personal and non-personal data?

- **Yes**
- No
- Not applicable

Please explain why not

Have restrictions on the location of data affected your strategy in doing business (e.g. limiting your choice regarding the use of certain digital technologies and services?)

- **Yes**
- No

Do you think that there are particular reasons in relation to which data location restrictions are or should be justifiable?

- **Yes**
- No

What kind(s) of ground(s) do you think are justifiable?

- **National security**
- **Public security**
- Other reasons:

Please explain

- The ‘free flow of information’ is fundamental to the working of the Digital Single Market in the future. Data localisation requirements disrupt the free flow and negatively impact industry. The free flow of data is paramount to cloud computing. So is the ability of cloud providers to host data where they deem best from a security, as well as from a financial point of view. Therefore, general sector or market wide data localisation laws and policies should be prevented or removed to avoid the risk of a fragmented internet.

- **Privacy & Security:** Localisation requirements are often introduced to avoid foreign surveillance and protect privacy and security of personal information against non-governmental criminal activities. However, data localisation does not ensure security per se. On the one hand, security depends on how companies protect their systems and continuously respond in best practice to the ever-growing sophistication of cyber criminals. Cloud business providers, for example, often take advantage of the Internet’s distributed infrastructure and use sharding and obfuscation techniques to avoid data being gathered in one place and thereby making it an ideal target for criminals and surveillance. On the other hand, security depends on the circumstances of the data centre itself (capacity, upgraded hardware, experienced security personnel to counter intrusions and detect signals associated with potential breaches, vulnerability to natural disasters). To sum up, access to the most advanced security technologies plays an important role. Localisation restrictions could limit the access by domestic companies to leading technology services in this area.

- **Economic Development:** Data localisation restrictions can often result in increased costs for businesses. For any service, it may not be economically viable to establish local servicers in certain territories. This applies in particular to SMEs (/start-ups) which are eager to attract customers not only domestically but also in a foreign market but do not have the budget to largely invest in expensive infrastructure. Especially in the cloud market, it is the ability to use the Internet to store data in the most cost-effective and secure location that supports scalability and drives efficiencies. Equally, for cloud users, localization measures reduce the offer and may limit the access to innovative products, which may not yet be offered in a specific location.

- **Public Procurement:** Public procurement policies, in particular, should explicitly allow for data transfers in Europe, and wherever possible, even outside of Europe, with all due safeguards as appropriate. Monitoring and enforcement should be in place to ensure individual public procurement exercises adhere to these principles.

- **Grounds from data localisation**: Limited exceptions in certain cases of national security and public security should be subject to stringent assessment and to the basic principles of necessity, proportionality, non-discrimination and subsidiarity. It is important to balance the impact of the policies on a country’s national security and public security with its potential impact on global trade, technology and innovation.

ON DATA ACCESS AND TRANSFER

Do you think that the existing contract law framework and current contractual practices are fit for purpose to facilitate a free flow of data including sufficient and fair access to and use of data in the EU, while safeguarding fundamental interests of parties involved?

Yes

No

Please explain your position

- As the digitisation of the European economy continues, data will increase in value. The shift to digital technology has enabled many consumers to store and share personal data, pictures, film, video images, etc. as well as companies to use such data for innovative business models. Existing EU law is well positioned to allow this fundamental transformation to proceed because it already provides for sufficient and fair access to and use of data in the EU, while safeguarding the fundamental interests of the parties involved.

- It is clear that the free flow of data cannot be without limits, as data remains subject to various sets of rules such as the E-Commerce Directive 2000/31 EC, the Consumer Rights Directive 2001/83/EC or the Data Protection Directive 95/46/EC. There is no need for new Regulation in this field. Every change of the existing legal framework will cause uncertainty and cost-intensive adaption processes and therefore should be limited to what is absolutely necessary. The focus should be on the harmonised implementation and enforcement of existing rules, as the identification of differences creates a high effort and cost for businesses.

- The trans-border free flow of data should not only be possible within the EU but also on a global scale as the Internet is also embedded in global environment. Sufficient mechanisms have been established in particular in the data protection field such as standard contractual clauses, BCRs or adequacy decisions by the Commission which safeguard consumer's interest while allowing for global trade.

In order to ensure the free flow of data within the European Union, in your opinion, regulating access to, transfer and the use of non-personal data at European level is:

Necessary

Not necessary

When non-personal data is generated by a device in an automated manner, do you think that it should be subject to specific measures (binding or non-binding) at EU level?

Yes

No

Which of the following aspects would merit measures?

Obligation to inform the user or operator of the device that generates the data

Attribution of the exploitation rights of the generated data to an entity (for example the person /

organisation that is owner of that device)

☐ In case the device is embedded in a larger system or product, the obligation to share the generated data with providers of other parts of that system or with the owner / user / holder of the entire system

☐ Other aspects:

Please specify

Please share your general comments or ideas regarding data access, ownership and use

- Trust and security in digital services is a key factor for the Digital Single Market. EU consumer and data protection rules must strike a balance between meeting the expectations of consumers while being fit for purpose for businesses. The current approach taken to update the EU data protection framework for the digital age already threatens to undermine the aspirations and vision of the DSM strategy. By creating greater legal uncertainty and more red tape across the Member States, as well as potentially establishing incentives for gathering more data than required, this could hinder the development of the DSM and European businesses and damage privacy and consumer confidence online

- **Non-personal data:** There is no need to introduce binding measures on these types of data. The existing data protection regime considers any data that may identify an individual as personal data. This wide definition of personal data ensures that individuals retain sufficient control over their data and allows them to protect their privacy. Moreover, the current definition of personal data is likely to be even further extended by the ongoing negotiations on the General Data Protection Regulation, providing individuals in the EU with even greater protection.

  Any new restrictions on data not covered by data protection regime should currently be avoided in order to deliver maximum benefit to the economy and society. They would represent real and more importantly unnecessary obstacles for any European business, small and big, to harness the new technological developments such as Big Data, Internet of Things or Industry 4.0. Generally, policymakers should monitor how new technology develops and establish an on-going dialogue with industry. Forward-thinking responses might be needed to deal with new issues in this field.

- **Data Ownership:** Ownership is a concept which applies to (material) things. Therefore, it is not fit for intangibles like data. In order to own a right for an intangible (for example a copyright) the owner has to make an effort. As long as the producer of non-personal data does not have such an effort it is not justified to grant him any rights for this non-personal data. Moreover the existing laws already know numerous rights for intangibles, which partly comprise rights of data. Adding a concept of data ownership would create conflicts with already existing rights.

- **Standardisation**: Global standards should be developed, for example in IoT, to enable discovery and interoperability of services on a worldwide basis. Bitkom generally supports continued voluntary action on interoperability and portability via global standards bodies and recommend limiting regulatory interventions on interoperability and portability to where there has been a finding of abuse of dominance. Mandatory rules on interoperability or portability would put a significant risk to IPR and innovation. The Commission should take as an example the

standardisation approach of the Web of the Things Interest Group. Beneficial in this regard could be the extension of research projects in this area with the aim of defining guidelines.

- All in all, the many different aspects of access to and use of non-personal data cannot be regulated beforehand by general law (especially hard laws). Such law would have to balance too many interests in an abstract manner and in doing so would paralyse the development of data-cooperation and new business-models based on data-analysis. The recent OECD Report on Data-driven Innovation for Growth and Well-being also highlights the complexity of these policy questions. The report suggests that policymakers should engage in further thinking on how issues of data ownership and the attribution of liability between decision makers, data and data analytics providers. It is commendable that the European Commission is committing to this thinking exercise and Bitkom would like to assist the Commission in its endeavour. By now, balancing the interests of different parties of data-cooperation should be left to and should be made possible for contract design.

ON DATA MARKETS

What regulatory constraints hold back the development of data markets in Europe and how could the EU encourage the development of such markets?

- **Fragmentation of data protection and copyright rules**: Fragmentation of data protection and copyright rules can be considered obstacles to the development of data markets.

- **Limits by rules for data protection and confidentiality:** In many cases data protection and confidentiality rules for personal data are an obstacle for the development of new business concepts. For example, they do not allow processing data about diseases in the cloud

---

ON ACCESS TO OPEN DATA

Do you think more could be done to open up public sector data for re-use in addition to the recently revised EU legislation (Directive 2013/37/EU)?

Open *by default means: Establish an expectation that all government data be published and made openly re-usable by default, while recognising that there are legitimate reasons why some data cannot be released.*

☐ **Introducing the principle of 'open by default'[1]**

☐ Licensing of 'Open Data': help persons/ organisations wishing to re-use public sector information (e.g., Standard European License)

☐ Further expanding the scope of the Directive (e.g. to include public service broadcasters, public undertakings);

☐ **Improving interoperability (e.g., common data formats);**

☐ **Further limiting the possibility to charge for re-use of public sector information**

☐ Remedies available to potential re-users against unfavourable decisions

☐ Other aspects?

Please specify

Access to open data will have a positive impact on the economy and society at large and opens potential for new products and services. Therefore, the Commission should focus on improving interoperability and introduce the principle of "open by default", further limit the possibility to charge for re-use of public sector information and make remedies available to potential re-users against unfavourable decisions.

Do you think that there is a case for the opening up of data held by private entities to promote its re-use by public and/or private sector, while respecting the existing provisions on data protection?

○ Yes

○ **No**

Under what conditions?

☐ in case it is in the public interest

☐ for non-commercial purposes (e.g. research)

☐ other conditions

Please explain

Data protection would not be the only aspect to be taken into account for the opening up of data held by private entities. In particular the interests of this private entity to protect its business secrets, its trade secrets and its know-how have to be taken into account. A general obligation for private entities to reveal data therefore cannot be supported.

ON ACCESS AND REUSE OF (NON-PERSONAL) SCIENTIFIC DATA

Do you think that data generated by research is sufficiently, findable, accessible identifiable, and re-usable enough?

○ Yes

○ **No**

Why not? What do you think could be done to make data generated by research more effectively re-usable?

Generally, data generated by research is sufficiently, findable, accessible identifiable, and re-usable.

However, another issue – in relation to research data, is the way copyright may impact text-and-data-mining activities. Access to material being mined should be secured - including, if appropriate, with a licence. But once access is acquired, there should be no additional

copyright permission required to mine the material, irrespective of whether the purposes are commercial or not. Exemptions in the US or Japan are already giving those countries a competitive edge, from research to business applications.

Do you agree with a default policy which would make data generated by publicly funded research available through open access?

- Yes
- **No**

Why not?

ON LIABILITY IN RELATION TO THE FREE FLOW OF DATA AND THE INTERNET OF THINGS

As a provider/user of Internet of Things (IoT) and/or data driven services and connected tangible devices, have you ever encountered or do you anticipate problems stemming from either an unclear liability regime/non –existence of a clear-cut liability regime?

*The **"Internet of Things"** is an ecosystem of physical objects that contain embedded technology to sense their internal statuses and communicate or interact with the external environment. Basically, Internet of things is the rapidly growing network of everyday objects—eyeglasses, cars, thermostats—made smart with sensors and internet addresses that create a network of everyday objects that communicate with one another, with the eventual capability to take actions on behalf of users.*

- Yes
- No
- **I don't know**

If you did not find the legal framework satisfactory, does this affect in any way your use of these services and tangible goods or your trust in them?

- Yes
- No
- **I don't know**

Do you think that the existing legal framework (laws, or guidelines or contractual practices) is fit for purpose in addressing liability issues of IoT or / and Data driven services and connected tangible goods?

- Yes
- No
- **I don't know**

Is the legal framework future proof? Please explain, using examples. (3000 characters maximum)

- **Liability today:** There already exist legal instruments governing liability of different actors. Examples include the E-commerce Directive that put in place a specific liability regime for services; or the data protection framework (95/46/EC).It is possible that future IoT innovations can challenge existing legal regimes (e.g. the autonomous car). Policymakers should monitor how such technology develops and establish an on-going dialogue with industry.

- **General position:** Forward-thinking responses might be needed to deal with new issues arising in this field. Currently, however, we do not see a need for new liability rules for data driven services and connected products. Hasty new legislation would do more harm than good.

Please explain what, in your view, should be the liability regime for these services and connected tangible goods to increase your trust and confidence in them? (3000 characters maximum)

- We currently see no need for a new or specific liability regime

---

As a user of IoT and/or data driven services and connected tangible devices, does the present legal framework for liability of providers impact your confidence and trust in those services and connected tangible goods?

- Yes
- No
- **I don't know**

In order to ensure the roll-out of IoT and the free flow of data, should liability issues of these services and connected tangible goods be addressed at EU level?

- Yes
- **No**
- I don't know

ON OPEN SERVICE PLATFORMS

What are in your opinion the socio-economic and innovation advantages of open versus closed service platforms and what regulatory or other policy initiatives do you propose to accelerate the emergence and take-up of open service platforms? (3000 characters maximum)

- **Definition:** The Commission should clarify what its understanding of “open platforms” since this is a broad concept which could be used to describe various services. Especially the distinction between “open” vs. “closed” service platforms is unclear:
  - If it means “open” for any consumer or reserved for “closed” user groups: There are no advantages for open platforms. Specific offers address specific needs. There is no reason why potential demand for services for closed user groups would not be met.
  - If “open” means without payment: there may be socio-economic advantages but there is no need for regulatory intervention in the market. Where socio-economic advantages exist but commercial offers do not meet the demand, public policy initiatives may provide such platform.
  - If “open” means open for competitive offers: there are socio-economic and innovative advantages of competition. Obligations for the non-discriminatory use APIs and standards, of Interoperability and portability can be optional instruments to reduce or revise competition dysfunctions. Policy initiatives can support techniques and standards which are open at fair, reasonable and non-discriminatory conditions.
- **General position:** There are benefits for both open and closed service platforms depending on the business model in question. A regulatory one-size-fits-all approach is therefore not possible. We not would encourage intervention into this diverse but fast moving market at this time.

PERSONAL DATA MANAGEMENT SYSTEMS

The following questions address the issue whether technical innovations should be promoted and further developed in order to improve transparency and implement efficiently the requirements for lawful processing of personal data, in compliance with the current and future EU data protection legal framework. Such innovations can take the form of 'personal data cloud spaces' or trusted frameworks and are often referred to as 'personal data banks/stores/vaults'.

Do you think that technical innovations, such as personal data spaces, should be promoted to improve transparency in compliance with the current and future EU data protection legal framework? Such innovations can take the form of 'personal data cloud spaces' or trusted frameworks and are often referred to as 'personal data banks/stores/vaults'?

- Yes
- No
- **I don't know**

Would you be in favour of supporting an initiative considering and promoting the development of personal data management systems at EU Level?

- Yes
- No

EUROPEAN CLOUD INITIATIVE

What are the key elements for ensuring trust in the use of cloud computing services by European businesses and citizens

"Cloud computing" *is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Examples of such resources include: servers, operating systems, networks, software, applications, and storage equipment.*

- **Reducing regulatory differences between Member States**
- **Standards, certification schemes, quality labels or seals**
- **Use of the cloud by public institutions**
- **Investment by the European private sector in secure, reliable and high-quality cloud infrastructures**

As a (potential) user of cloud computing services, do you think cloud service providers are sufficiently transparent on the security and protection of users' data regarding the services they provide?

- Yes
- No
- **Not applicable**

What information relevant to the security and protection of users' data do you think cloud service providers should provide?

- **Current framework:** Cloud service providers are already sufficiently regulated with regard to security and protection of users' data. When cloud service providers process personal data, they are already fall under the transparency requirement of the 95/46/EC and will be subject to similar requirements under the General Data Protection Regulation. Similarly, in the ongoing negotiations on the NIS Directive cloud service providers will face new additional security obligations, notably on reporting of security breaches.

- **Information policy:** There should be generally transparent information about data access, use of data, responsible entities, certifications, etc. Furthermore, cloud service providers should make clear which measures they take in order to secure and protect user's data. The users should be aware of the level of protection they need and should be able to choose a supplier accordingly.

- **Cloud SiG, Data Privacy Code of Conduct:** The Cloud SiG Data Privacy Code of

Conduct, which sets out data protection and security objectives and principles for cloud service providers, should be also finalized.

As a (potential) user of cloud computing services, do you think cloud service providers are sufficiently transparent on the security and protection of users' data regarding the services they provide?

Yes

No

Not applicable

As a (potential) user of cloud computing services, do you agree that existing contractual practices ensure a fair and balanced allocation of legal and technical risks between cloud users and cloud service providers?

Yes

No

Please explain

- Fair practice in the current contractual practices in cloud computing market: We believe that current contractual practices ensure a fair and balance allocation of legal and technical risks.

- **Current framework B2C:** When providing services to a consumer, a provider of cloud computing services just like any other provider of consumer services may use General Terms and Conditions of use. The Directive on unfair terms in consumer contracts ensures that consumers are more than sufficiently protected against unfair terms. EU member states have implemented effective means under national law to enforce these rights and that invalid terms are no longer used by businesses. In addition Directive 95/46/EC reduces technical risks for consumers as it obliges providers of cloud services to implement appropriate technical and organizational measures to protect consumers' personal data against accidental or unlawful destruction or 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. It is not possible for a cloud service provider to set forth contractual terms below this high standard of security.

- **Current framework B2B**: In the business to business 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). These contracts are not based on a take it or leave it approach, they are formulated and adapted to suit user requirements while minimising the need for lengthy individual negotiations and legal costs. Cloud service providers are also subject to the security requirements of Directive 95/46/EC and will be under similar requirements under the GDPR. 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 for their data.

What would be the benefit of cloud computing services interacting with each other (ensuring interoperability)

☐ **Economic benefits**

☐ **Improved trust**

☐ **Others:**

Please specify

- **Benefit for the market**: Interacting, cooperation and interoperability maximise economies of scale through efficient use infrastructure, standardisation of interfaces and more efficiency for interconnected processes. Interoperability maximise the positive network effect and opens it to all interacting providers. It also reduces the risk of monopolisation the network effect by one provider. Interacting can increase the security of cloud services because of raising transparency, specifically through the level of coordination sharing between cloud service providers on technical and safety matters. This helps to build trust and strengthens resilience of the entire value chain. However, it can also increase the risk for the security of cloud services because of possible impact of breach of security of one provider for interacting providers.

- **Benefit for Consumers:** The ability to switching between platforms allows users to opt for the service which is most appealing to them or use a multi-cloud strategy, making the market more competitive, and driving innovation. Cloud interoperability avoids lock-ins and assures maximum freedom and flexibility for consumers.

- **Standardisation:** Standards should be developed at a global level, to ensure true global interoperability, especially in order for local economies to benefit from global markets. In this context, it is worrisome that the Commission might use its mandate to push for the development of European standards. Such European standards would rather compete than complement other global standards for digital services.

What would be the benefit of guaranteeing the portability of data, including at European level, between different providers of cloud services

☐ Economic benefits

☐ Improved trust

☐ Others:

Please specify

Have you encountered any of the following contractual practices in relation to cloud based services? In your view, to what extent could those practices hamper the uptake of cloud based services? Please explain your reasoning.

	Never (Y[es] or N[no])	**Sometimes** (Y / N)	**Often** (Y / N)	**Always** (Y / N)	**Why?** (1500 characters max.)
Difficulties with negotiating contractual terms and conditions for cloud services stemming from uneven bargaining power of the parties and/or undefined standards					
Limitations as regards the possibility to switch between different cloud service providers					
Possibility for the supplier to unilaterally modify the cloud service					
Far reaching limitations of the supplier's liability for malfunctioning cloud services (including depriving the user of key remedies)					
Other (please explain)					

What are the main benefits of a specific European Open Science Cloud which would facilitate access and make publicly funded research data re-useable?

- ☐ **Making Science more reliable by better quality assurance of the data**
- ☐ **Making Science more efficient by better sharing of resources at national and international level**
- ☐ **Making Science more efficient by leading faster to scientific discoveries and insights**
- ☐ **Creating economic benefits through better access to data by economic operators**
- ☐ **Making Science more responsive to quickly tackle societal challenges**
- ☐ **Others**

Please specify

Would model contracts for cloud service providers be a useful tool for building trust in cloud services?

Yes

No

Would your answer differ for consumer and commercial (i.e. business to business) cloud contracts?

Yes

No

What approach would you prefer?

- In principle, model contracts can help enterprises, especially SME-cloud-suppliers to be compliant with consumer law and with contract law.

- **Difficulty with model contracts in this area**: The probably insurmountable difficulty with cloud model contracts is the great variety of business models and cloud offers including hosting-, communication-, computation-, content- and collaboration-services. As a consequence a model contract would seldom be applicable to a given cloud offer without adaptions. If adaptions are necessary for a special contract the value of a model contract diminishes substantially. Moreover, the copyright laws in the EU are not sufficiently harmonised to use standard contract terms for licencing software-rights in cloud contracts.

- The reasons why one unifying model contract for cloud services seems unfeasible and inappropriate apply equally to consumer and commercial cloud contracts.

Please share your general comments or ideas regarding data, cloud computing and the topics addressed in this section of the questionnaire

Europe will be best prepared to face the digital disruption of the future if the legislative and regulatory framework is right:

- **Data Transfers and localization measures**: International data transfers need to remain possible. Data localisation measures should be limited to what is strictly necessary and proportionate.

- **Interoperability and portability**: We support continued voluntary action on interoperability and portability via global standards bodies and recommend limiting regulatory interventions on interoperability and portability to where there has been a finding of abuse of dominance. Otherwise there is significant risk to IPR and innovation.

- **Co-Regulation and certification**: The current model for industry self-regulation works well. Regulation should be achieved through market dynamics. Examples for good initiatives are e.g. the Cloud SiGs – which provides useful guidance for cloud adopters on appropriate certification schemes and applicable standards.

- **Regulatory restraint**: Europe is not known for insufficient regulation, rather the

opposite. Too strong and too prescriptive regulation risks slowing down digitalization and new business models in this field rather than fostering them. The aim should be to reduce and further harmonize the regulatory burdens for platforms and for the collaborative economy.

The collaborative economy

The collaborative economy

The following questions focus on certain issues raised by the collaborative economy and seek to improve the Commission's understanding by collecting the views of stakeholders on the regulatory environment, the effects of collaborative economy platforms on existing suppliers, innovation, and consumer choice. More broadly, they aim also at assessing the impact of the development of the collaborative economy on the rest of the economy and of the opportunities as well as the challenges it raises. They should help devising a European agenda for the collaborative economy to be considered in the context of the forthcoming Internal Market Strategy. The main question is whether EU law is fit to support this new phenomenon and whether existing policy is sufficient to let it develop and grow further, while addressing potential issues that may arise, including public policy objectives that may have already been identified.

Terms used for the purposes of this consultation:

"Collaborative economy"

For the purposes of this consultation the collaborative economy links 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. Typical examples are transport services including the use of domestic vehicles for passenger transport and ride-sharing, accommodation or professional services.

"Traditional provider"

Individuals or legal persons who provide their services mainly through other channels, without an extensive involvement of online platforms.

"Provider in the collaborative economy"

Individuals or legal persons who provide the service by offering assets, resources, time, skills or capital through an online platform.

"User in the collaborative economy"

Individuals or legal persons who access and use the transacted assets, resources, time, skills and capital.

Please indicate your role in the collaborative economy

- ☐ Provider or association representing providers
- ☐ Traditional provider or association representing traditional providers

- [ ] **Platform or association representing platforms**
- [ ] Public authority
- [ ] User or consumer association

Which are the main risks and challenges associated with the growth of the collaborative economy and what are the obstacles which could hamper its growth and accessibility?

Please rate from 1 to 5 according to their importance.

- Not sufficiently adapted regulatory framework

- ( ) **1**
- ( ) 2
- ( ) 3
- ( ) 4
- ( ) 5

- Uncertainty for providers on their rights and obligations

- ( ) **1**
- ( ) 2
- ( ) 3
- ( ) 4
- ( ) 5

- Uncertainty for users about their rights and obligations

- ( ) **1**
- ( ) 2
- ( ) 3
- ( ) 4
- ( ) 5

- Weakening of employment and social rights for employees/workers

- ( ) **1**
- ( ) 2
- ( ) 3
- ( ) 4
- ( ) 5

- Non-compliance with health and safety standards and regulations

1

2

3

4

5

- Rise in undeclared work and the black economy

1

2

3

4

5

- Opposition from traditional providers

1

2

3

4

5

- Uncertainty related to the protection of personal data

1

2

3

4

5

- Insufficient funding for start-ups

1

2

3

4

5

- Other, please explain

- Insufficient funding is by far not the only problem for start-ups in Europe: the regulatory framework and the political climate regarding the digital economy have to be improved, in

order to support the growth of start-ups in Europe

- New regulation often seeks to target large and established platforms but eventually hits smaller platforms and start-ups

- Innovation, which is often made possible by platforms (e.g Apple App Store, Google Maps) is hampered by insecurity regarding regulation and a political climate of platform skepticism and anti-platform campaigns.

How do you consider the surge of the collaborative economy will impact on the different forms of employment (self-employment, free lancers, shared workers, economically dependent workers, tele-workers etc) and the creation of jobs?

- **Positively across sectors**
- Varies depending on the sector
- Varies depending on each case
- Varies according to the national employment laws
- Negatively across sectors
- **Other**

Please explain

Digital platforms and the collaborative economy have a positive effect on employment across sectors and the various types of employment. A few examples and figures to support this claim:

- In 2011 Facebook commissioned Deloitte to estimate its economy impact across the then 27 member states of the EU and Switzerland. The central estimate of gross revenue enabled by the activities of Facebook is 32 billion EUR. This revenue converts into an economy impact of 15.3 billion EUR and supports 232,000 jobs (Deloitte: Measuring Facebook's economic impact in Europe, January 2012).

- Europe has a very large and vibrant app producing industry which generates significant revenues and jobs. These revenues and jobs exist solely because of the widespread popularity of smartphone platforms such as Apple iPhone / iOS / App Store or Google Android / Play Store. According to a study commissioned for the European Commission, the EU-wide app-developer workforce will grow from 1 million in 2013 to 2.8 million in 2018. Additional support and marketing staff result in total app economy jobs of 1.8 million in 2013, growing to 4.8 million in 2018 (Gigaom Research:Sizing the EU app economy, 2014). Concerning the collaborative economy, an even greater economic contribution of smartphone platforms is the enablement of apps for passenger transport and ride-sharing, accommodation or professional services which then subsequently are able to generate jobs themselves.

Do you see any obstacle to the development and scaling-up of collaborative economy across borders in Europe and/or to the emergence of European market leaders?

- **Yes**
- No

Please explain

- We support the goal of the Digital Single Market strategy to curb digital sectionalism in Europe. However, this goal should be reached by harmonizing existing rules and standards not by creating more regulation.

- Because their international user communities collaborative economy companies are often hampered by the lack of EU-wide standards. For example there is no EU-wide definition of what constitutes a freelancer.

Do you see a need for action at European Union level specifically to promote the collaborative economy, and to foster innovation and entrepreneurship in its context?

Yes

No

Please indicate the sector/action

- We do not see the need for EU funding programs regarding the collaborative economy that aim to establish “neutral” platforms. The development of collaborative economy platforms should be left to the corporate sector and should take place according to market laws.

- We do however see the need for more and better structured action by the EU regarding open data, start-ups and education for the digital age.

- We plead for a start-up friendly and harmonized regulatory framework within the EU. Especially regarding the data protection directive, the interests of start-ups have to be considered and trust in innovative business models has to be improved.

What action is necessary regarding the current regulatory environment at the level of the EU, including the Services Directive, the E-commerce Directive and the EU legislation on consumer protection law?

No change is required

New rules for the collaborative economy are required

More guidance and better information on the application of the existing rules is required

I don't know what is the current regulatory environment

Please indicate the sectors and the rules concerned

- Better harmonization of standards and laws within the EU, especially regarding consumer protection rights and law.

- A strengthening of consumer autonomy within the EU’s regulatory environment.

- A political climate within EU institutions that promotes innovation instead of hampering it.

Thank you for your contribution