SYNOPSIS REPORT ON THE CONTRIBUTIONS TO THE PUBLIC CONSULTATION REGULATORY ENVIRONMENT FOR DATA AND CLOUD COMPUTING

Contents

1. EXECUTIVE SUMMARY

The Commission carried out a web-based public consultation on platforms, on liability of intermediaries, on data and cloud, and on the collaborative economy from 24 September 2015 to 6 January 2016. Out of the 1005 replies received through the EU-Survey, 653 replies were on the data and cloud section of the consultation.

The feedback received from the consultation shows that data location restrictions are affecting respondents' use of data services and affecting business strategies, and action is needed. While the majority of respondents also consider that there are some justifiable grounds for data location restrictions under strict rules, such as national and public security, business respondents emphasized that data location restrictions can be a barrier to the development of the data economy and the competitiveness of industry in Europe. It was also pointed out that restrictions on data location could increase data security risks.

The majority of respondents consider that the existing legal framework and contractual practices for access to and use of data are not fit for purpose in the EU. While consumer groups and individual citizens clearly support the need for legal clarity, just over 50% of business respondents (including a significant group of business users) also feel the current framework on access and use is not fit for purpose to facilitate the free flow of data. Many of the businesses that view the contract law framework positively are providers of data services and technologies, who put a greater emphasis on maintaining contractual freedom as regards ownership of non-personal data. Some indicated difficulties in distinguishing between personal and non-personal data (but a number of these replies focused on international data transfers, which are outside of the scope of the consultation and of the planned initiative).

Respondents identified a number of constraints that hold back the development of data markets in Europe, and there was acceptance of the need for legal certainty in order to stimulate investment. While there was no clear consensus on what measures to take, nearly two thirds of those in favour of specific measures support steps to attribute the exploitation rights of data generated by a device in an automated manner. Business respondents tend to favour soft measures that facilitate business opportunities in the context of emerging data markets, and guidance in relation to legal uncertainties regarding access and use.

Almost half of the respondents have encountered or anticipate problems stemming from an unclear liability regime in relation to data and the Internet of Things. A majority of individual citizens and consumer associations think that the present legal framework for liability is not satisfactory and thus impacts their confidence and trust in IoT and data services. The overall majority of respondents confirmed that there is a need for action to address liability issues for IoT services at EU level in order to ensure the roll out of these services and the free flow of data. Additionally, almost two thirds of users consider the regulatory framework to be unsatisfactory.

With regard to the European Cloud initiative, respondents consider security and protection of users' data critical. Cloud service providers and users (including business users) have opposing views on transparency and fair contractual practices. Cloud users are sensitive about the protection of their data and consider that contractual terms lack transparency. Cloud providers, on the other hand, consider that their contract terms are sufficiently transparent and fair and that users are sufficiently protected by EU law.

According to the respondents, interoperability issues and the introduction of the principle of "open by default" for public sector data are the main areas for improvement as regards open access to data. More than four fifths of respondents (including replies from all categories of respondents) consider that data generated by research is not sufficiently accessible and re-usable and therefore support a default "Open Science" policy to make data generated by publicly funded research available through open access.

The majority of respondents recognise the economic benefits of action to ensure interoperability and data portability (particularly to facilitate switching of provider). Many respondents consider that a self-regulatory approach would be more appropriate with regards to cloud-based services, and that model contracts could be a useful tool for building users' trust. Respondents also see specific benefits coming from a European Open Science Cloud, which would facilitate access and make publicly funded research data accessible and re-usable.

2. INTRODUCTION

As part of its broader analysis of the role of platforms in the economy and society, as announced in the Digital Single Market Strategy for Europe in May 2015, the Commission carried out an online public consultation from 24 September 2015 to 6 January 2016. The consultation sought to gather evidence and views on the regulatory environment for platforms, on liability of intermediaries, on data and cloud, and on the collaborative economy, with individual sections for these respective themes.

This current report addresses only the outcome of the consultation on the data and cloud in digital ecosystems section. The objective of this section of the consultation was to seek views and collect EU citizens' and businesses' needs and expectations on the forthcoming European Cloud initiative and the European Free Flow of Data initiative.

The consultation was published in 24 languages on the Commission's websites and further promoted through social media channels, stakeholder meetings, etc. A summary report on the first results of the public consultation was published on 26 January 2016.

With the exception of the demographic questions at the beginning of the questionnaire, replies to questions in the individual sections of the public consultation (including the data and cloud section) were optional. Respondents often chose not to answer all the questions and hence not all sections of the public consultation. Therefore, where figures are reported below, these derive from respondents who replied to that particular question. Those who did not reply to a specific question are not accounted for in the figures presented. This is to ensure clarity with regard to the interpretation of the data.

The figures used to describe the distribution of responses derive from the answers provided under the EU-Survey tool. Over 50 written submissions were also received from stakeholders, such as position papers and contributions by email, and these have been taken into account when describing and analysing the views of stakeholders, but were not considered for the statistical representation.

In addition, the Commission has engaged with stakeholders through the Cloud-Select Industry Group[1], and organised a roundtable on emerging issues on ownership, access and reusability of data in March 2016. Further meetings with stakeholders will be organised following the publication of this report and of the Inception Impact Assessment report on the Free Flow of Data initiative to be published shortly.

3. OVERVIEW OF RESPONDENTS TO THE PUBLIC CONSULTATION

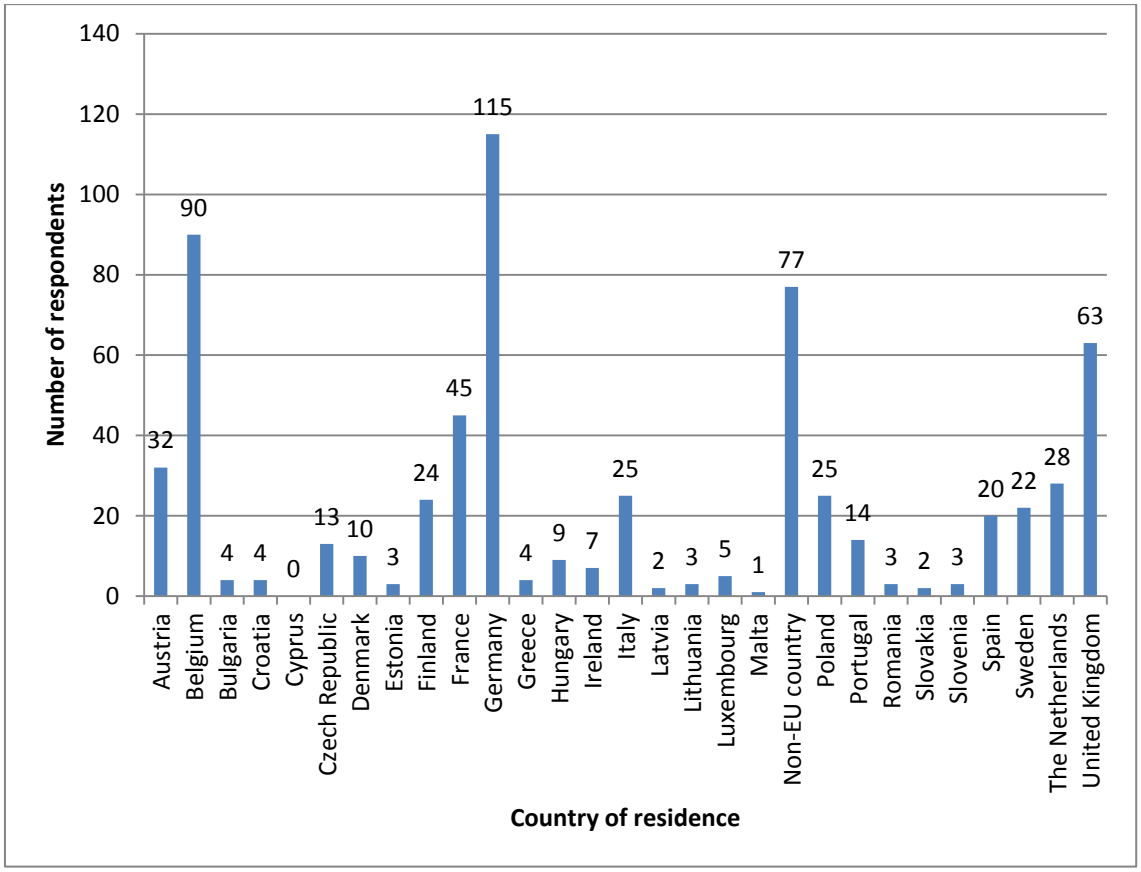
The public consultation on the regulatory environment for platforms, on liability of intermediaries, on data and cloud and on the collaborative economy received 1034 replies, 1005 of which were submitted through the EU-Survey, and 29 through the functional mail box set up exclusively for the consultation. Not all respondents replied to all four sections. The section on data and cloud received 653 replies.

The breakdown of type of respondent to the data and cloud section is as follows:

[1] The last plenary meeting of the Cloud-Select Industry Group took place on the 29th of October 2015. The meeting report is available here: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=12638

Type of respondent	Number of replies
Business	83
Public authority	18
Research institution or think tank	24
Business associations	114
Civil society organisations	28
Consumer associations	10
Individual citizen	304
Online platform	28
Other	44
Total	653

As to the geographical distribution of responses, replies came from almost all EU Member States. The breakdown of the replies to the data and cloud section per Member States is as follows:



4. ANALYSIS OF THE RESPONSES

4.1. Data location restrictions

4.1.1. Measures to make a clear distinction between personal and non-personal data in the context of the free flow of data in the EU

A majority of respondents across almost all respondent groups (including businesses and SMEs) make a distinction between personal data and non-personal data. Most of those

who do not make a clear distinction in practice stress that this is due to the fact that, depending on the services offered, they have limited or no access to the data within specific workloads of the customer and that data classification may have been carried out by entities other than the service providers (including end customers). Moreover, even if it is possible to make such distinction, both sets of data are likely to be subject to the same contractual obligations.

Almost all the individual citizens who contributed have either expressed their doubts as to the relevance of the distinction between personal and non-personal data ("*the lines are blurry*", "*unclear line between the two*", "*no black/white difference*") or have asserted that all data should be considered as personal.

4.1.2. Have restrictions on the location of data affected your strategy in doing business?

Two thirds of respondents across all respondent groups consider that restrictions on the location of data have affected their strategy in doing business.

4.1.3. On the particular reasons in relation to which data location restrictions are or should be justifiable

A majority of respondents across almost all groups, with the exception of think thanks, believe that there are justifiable grounds for some data location restrictions. The grounds considered legitimate are equally shared between "national security", "public security" and "other reasons" across different groups of respondents.[2]

Most of the respondents who consider that national security or public security can be justifiable grounds for some form of data location restrictions highlight that such restrictions should be assessed strictly (i.e. should be limited to sensitive governmental powers) in order to avoid undue restrictions to the development of the DSM. Respondents claim that the restrictions would be justified only if limited to issues related to national sovereignty. Any restrictions should also be applied to the DSM as a whole to prevent singular national approaches that would disrupt the market. In order to ensure that data location restrictions are assessed strictly, some respondents claim that a procedure for data classification should be established to provide guidance on what kind of data must be stored locally.

Some respondents assert that data location restrictions can increase data security risks by requiring the storing of data in a single centralised location that can be vulnerable to natural disasters or intrusions, as well as being a more attractive target for state surveillance. This opinion is shared by businesses and civil society. They emphasise that data location restrictions are inconsistent with the borderless nature of the Internet.

Business respondents generally emphasize that data location restrictions may be a barrier to the development of the data economy in Europe and the competitiveness of the European industry in this field. They also underline the importance of the freedom of contract regarding data location restrictions in the private sector.

---

[2] This question appears to have been understood differently by the stakeholders. Several respondents found the concept of "data location restrictions" unclear, and wondered whether the question was considering restrictions within the EU or worldwide. Therefore some responses do not make it clear whether they are concerned about restrictions to data flows between Member States or restrictions to data flows between the EU and third countries, which is a rather different issue.

Among the "other reasons", the majority of respondents (including respondents from the business sector, public authorities and almost all individual citizens), invoke “privacy” or “data protection” as a justifiable ground for data location restrictions. However, most of the concerns expressed are unambiguously related to international transfers of data towards third countries, rather than transfers of data within the EU, where strong personal data protection rules apply. Among business respondents, this can be understood as a way of ensuring compliance with EU General Data Protection Regulation. Individual citizens also stress the risks related to transfers of data outside the EU territory.

Businesses respondents also invoke the protection of trade secrets, the protection against economic espionage, the protection of competition, or the protection of intellectual property as justifiable grounds for data location restrictions without specifying whether they are concerned by transfers within the EU or with third States.

4.2. Data access and transfer

4.2.1. 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 the fundamental interests of parties involved?[3]

Most of the replies are related to personal data protection issues (especially international data transfers) and express concerns in relation to fundamental rights of users and lack of transparency in relation to law enforcement access to personal data. Some respondents (business and individual citizens as well) highlighted the difficulties to define the scope of this question (personal or non-personal data) and also difficulties to define non-personal data (see also 4.1.1).

The opinion of business respondents regarding the adequacy of the current contract law framework applicable to data flows in the EU is rather divided.

Among businesses that assess the existing contract law framework as not fit for purpose, a majority point out the insufficient harmonisation of legislations between the Member States, in particular data protection legislations. They usually call for more harmonization at EU level, and rapid adoption of the General Data Protection Regulation and future e-Privacy Directive. The second most important trend here relates to the contractual model applicable to international transfers, in particular transatlantic data transfers, and the fact that it remains too cumbersome for businesses, and also that the new Data Protection Package does not address the specific issue of transatlantic transfers of data (the consultation closed before the Privacy Shield agreement was announced).

Among those business respondents who assess the current contract law framework positively, including a significant number of providers of business technologies and services, the majority are explicitly against the adoption of any additional regulation in this matter, claiming that the legal framework has proven to be sufficient, although some favour a more consistent application of the rules within the EU. Some of them insisted further on the importance of maintaining the freedom of contract and competition

[3] This question appears to have been understood differently by the stakeholders. Some respondents were not sure whether the question was related to the free flow and use of personal data or non-personal data. Moreover, although the question refers explicitly to data flows “in the EU”, many contributions from all respondent groups have here again included comments regarding international data transfers, in particular the transatlantic data transfers.

presently in place. As such, the adoption of the General Data Protection Regulation (GDPR) is perceived as a positive step towards facilitating data flows in the EU, as well as a way to address the diversity and sometimes contradictory data protection requirements in different EU Member States.

Among associations representing consumers and civil society, as well as research institutions and think tank groups respectively, one third have a positive opinion of the existing contract law framework, and two thirds have a negative opinion, with no identifiable trends among the two groups.

Among individual citizens, around two fifths of them have a positive opinion of the legal framework, while three fifths have a negative opinion. Half of the respondents with a positive opinion say that they have not experienced any particular problems and that the data protection laws in place are sufficient. Among respondents who have a negative opinion of the current legal framework, the primary issue raised is related to state surveillance (e.g. by intelligence services), as well as insufficient harmonization of EU law, in particular data protection law.

On the other hand, a majority of public authorities have a positive opinion of the current framework.

4.2.2. Regulating access to, transfer and the use of non-personal data at European level in order to ensure the free flow of data within the European Union

The majority of respondents consider that it is not necessary to regulate access to, transfer and the use of non-personal data at European level, including a significant number of providers of business technologies and services. Respondents from the public sector are however divided on the necessity to regulate and no conclusive trend can be identified. Only a handful of countries are in favour of a regulation; few are clearly against regulation. Other Member States are either not taking a clear position or did not respond to the survey.

4.2.3. Specific measures (binding or non-binding) to automatically generated non-personal data[4]

There is no clear consensus among the respondent groups whether non-personal data automatically generated by devices should or should not be subject to specific measures (in a binding or non-binding way).

Nevertheless, a majority of business groups are against specific measures, claiming that any new restrictions on data not covered by the (personal) data protection regime should be avoided in order to deliver maximum benefit to the economy and society. On the other hand, most respondents among consumers and civil society associations, and a majority of business users support specific measures on automatically generated non-personal data.

When specific measures are considered necessary, almost all respondents highlight the obligation to inform the user or operator of the device that generates the data. The

[4] The differentiation between personal data and non-personal data is considered as a problematic issue by some respondents, from different categories - the notion of non-personal data is not sufficiently clear.

majority of respondents consider that (i) *attribution of the exploitation rights of the generated data to an entity*, and (ii) *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*, merit measures. Regarding *other aspects*, most of the replies call for the respect of personal data protection issues, such as transparency, consent, data portability and anonymisation of personal data.

4.2.4. General comments or ideas regarding data access, ownership and use

Regarding the need for regulation of ownership issues of non-personal data, many business respondents referred to the absence of proof of market failure. Their primary concern was to maintain contractual freedom due to the complexity and uniqueness of each processing situation, as well as a fear that possible regulation could stifle innovation and impede the development of the market. Businesses also consider that the existing regime of data protection laws deal adequately with issues of ownership, use and access regarding personal data. They encourage the Commission to further explore this complex issue for non-personal data. On the other hand, no major trend can be derived from consumers, civil society associations, as well as research institutions, think tanks and individual citizens.

4.3. Data markets

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

The respondents identified a number of issues perceived as regulatory constraints to the development of data markets:

- There was consensus among respondents that trust and privacy concerns of data subjects are of primary importance and in that respect the General Data Protection Regulation amounts to a cornerstone.

- Existing data localisation requirements have also been identified as a blocking factor making cross-border data transfers and (re)use of data difficult or impossible.

- Several respondents pointed out that excessive copyright terms represent obstacles to functional data markets by locking up data by copyright holders.

- Some respondents underlined the importance of stronger intermediary liability exemptions for the purpose of creating data markets while decreasing the restrictions on emergent business models arising from the novel use of existing content and technology.

- Further EU efforts facilitating access to non-personal data, use and re-use of data were also mentioned as an important factor by respondents.

Respondents emphasised that data and data markets need to be treated as economic assets that are crucial for EU competitiveness and prosperity. The European Commission was encouraged to work on codes of conduct and certification schemes that facilitate business opportunities in the context of emerging data markets.

Finally, some of the replies brought to light other potential blocking factors that are non-regulatory in nature, but which seem to represent challenges from the point of view of developing data markets. Commercial considerations (e.g. compliance requirements, profitability, market demand), language barriers or diverse taxation rules across EU Member States were mentioned.

4.4. Access to open data

4.4.1. 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)?

The largest number of answers pointed at interoperability issues (such as common metadata formats) as the main area for improvement alongside the need to introduce the principle of "open by default". The second factor most often cited by respondents was excessive charging for the re-use of data while the third most common reply focused on licensing (indicating that current licensing solutions and available support to organisations wishing to re-use public sector data was insufficient).

The open question yielded a mix of replies, with two topics arising more frequently than others:

- Copyright: several respondents indicated that the PSI re-use regimes should not be used to undermine the protection awarded by intellectual property rights, particularly in the field of broadcasting material and in the cultural heritage sector.

- Interoperable licensing: some replies suggested that an adoption of an international licensing standard in its most liberal option (such as CC0[5]) might be necessary to boost re-use of PSI in the EU.

A vast majority of respondents (around three quarters) have indicated their desire for the "open by default" principle to be introduced. Several citizens justify this by saying that what taxpayers have supported should be mandatorily open by default and freely available.

Moreover, some respondents have indicated that the "open by default" principle could not be set up in contradiction with existing intellectual property rights.

A limited number of the respondents have pointed out to "licensing of open data" as a means of reinforcing the possible re-use of PSI. SMEs show the greatest interest in developing standard licenses.

The idea of further expanding the scope of the PSI Directive (e.g. to include public service broadcasters, public undertakings) has received moderate support. A contrast appears between businesses, trade associations, online platforms and SMEs who have shown pretty low support for this proposition and individual citizens, consumer associations, research institutions and think tanks who favour it.

[5] https://wiki.creativecommons.org/wiki/CC0

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

The question on the need for opening up data held by private entities to promote its re-use by the private and or public sector provided mixed results depending on the nature of the stakeholders.

Around half of the answers coming from businesses, trade association representing businesses and online platforms were negative.

The public authorities gave a mixed answer: while the majority of them did not answer the question, one third of the public authorities responded favourably to the question.

The majority of research institutions, civil society associations, consumers associations and individual citizens gave a positive answer.

As regards the conditions under which such re-use of data should be taking place, the results were generally equally broken down between the public interest and non-commercial purposes. From the business perspective, given the generally negative answer given to the previous question, a great proportion of respondents from the business sector did not provide any answer.

The follow-up open replies yielded some interesting (albeit scarce) opinions on that matter:

(1) Public funding means openness: several respondents (mostly individuals) recommended that any data generated with public money must be made openly reusable. In particular, utility companies were singled out in this context.

(2) Data used for commercial standards: a few replies indicated that whenever privately held data support the creation of commercial standards that are incorporated into law, such as building codes, there is a strong case to be made for public open access to both the standard and the underlying data that led to its incorporation in law.

(3) Some replies (mostly companies and trade associations) suggested that at the current stage of the data economy, private entities should be encouraged to build data markets rather than have data taken away from them. There should be no regulatory requirement to share but on the contrary, conditions should be put in place to encourage sharing of data amongst private actors as well as between private and public actors.

4.5. Access and reuse of (non-personal) scientific data

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

A large majority of respondents (approximately four fifths) consider that data generated by research is not sufficiently findable, accessible, identifiable, and re-usable ("fair").

Among respondents, individual citizens show the strongest support for open research data. More than four fifths of respondents consider that research data is not sufficiently accessible and re-usable.

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

A large majority of respondents (around four fifths) support a default policy that would make data generated by publicly funded research available through open access. Among all respondents, around 9 out of every 10 of individual citizens support open access by default to public research data.

Replies from businesses and business associations in relation to open access agreed with a default policy which would make data generated by publicly funded research available through open access. The questions of openness of public research data were among the ones that were answered by most participants (fewer 'no answer'). To a large extent, this further indicates that these specific issues are of great importance for all stakeholders, including individual citizens. These results strongly back the Commission's resolve to further open up publicly funded research data and it also gives a strong signal to other national and international research funders.

4.6. Liability in relation to the free flow of data and the Internet of Things

4.6.1. As a provider/user of 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?

Among all the respondents (gathering both providers and users, including individual users, of IoT data driven services), almost half of them claim to have encountered problems or they anticipate problems stemming from a liability regime for these types of products and services that they consider unclear, while nearly a quarter declare not to be able to answer the question, and almost a third declare not to have encountered or not anticipating any problem stemming from the liability regime. Content providers and intermediaries are the two respondent groups which expressed the greatest concerns with regards to the liability regime.

Almost half of the respondents (gathering both providers and users of IoT data driven services), claim not to have found the legal framework satisfactory, and state that it has impacted the use of these IoT services and tangible goods, and affected the trust users have towards it. On the users' side almost two thirds, and on the provider side around one third, of the respondents find the regulatory framework not satisfactory.

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

There are quite divergent views expressed in the consultation in relation to liability issues. A majority of the overall respondents (including individuals and businesses) take the view that the existing legal framework (laws, guidelines or contractual practices) is not fit for purpose to address liability issues of IoT and/or data driven services and connected tangible goods. From the responses, it appears that this affects the use of these services and goods, as well as users' trust in them. The responses however do not allow to identify trends as regards the identification of which instruments in the existing legal framework are not fit for purpose and why.

There was considerable divergence in the replies coming from businesses and business trade associations (including platforms). Two fifths of respondents in this category are of the opinion that the existing legal framework is fit for purpose in addressing liability issues for IoT data driven services and connected tangible goods, while less than a third are of the opinion that it is not fit for purpose. At the same time however, almost half of the individual users do not believe that the existing legal framework is fit for purpose.

Some individual citizens pointed out the potential harm to innovation following ex ante or a priori regulation of technology that has not been fully developed and deployed yet. The implementation of such a framework might constitute barriers, hold back innovation and lock-in inefficiencies. Most of the individual citizens argued that the current legal framework itself is future proof due to its discretion/ambiguity while regulations attempting to govern this emerging area are not future proof and adaptable to technological innovations. The big danger in regulating new and emerging technologies is that progress and change is happening very rapidly in this area and introducing any set of specific regulations would slow down this innovation, and the regulations are likely to become obsolete as products and services continue to evolve.

The vast majority of the respondents from businesses or business trade associations pointed out that the liability risks discussed in the framework of IoT are technology neutral. Businesses also confirmed that there are already various legal instruments governing liability of different actors in place (e.g. the E-commerce Directive, EU data protection rules and the Product Liability Directive). The right balance between the interests of the stakeholders affected must be provided for and the regulatory framework must remain technology neutral.

Several organisations mentioned the recommendation from the AIOTI WG4 that underlines that when developing policy solutions a close dialogue between policy-makers and industry should take place.

4.6.3. What should be the liability regime for these services and connected tangible goods to increase trust and confidence in them?

Most of the respondents, a majority of them businesses and business or trade associations, do not see the need for a new or specific liability regime, because they believe that the current framework is sufficiently technology neutral. It was also emphasised by many respondents that there is nothing intrinsically different about the IoT that calls into question existing liability regimes governing liability of different actors. Some respondents pointed out that the technology in this area has been developing much faster than legislation, thus some legislation needs to be reviewed, clarified and in some cases adjusted in the light of emerging IoT value chains. In that respect, respondents referred in particular to the data protection legislation.

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

The majority of individual citizens and consumer associations believe that the present legal framework for liability impact their confidence and trust in those services. An even higher number of business and business trade associations confirm that the present framework for liability impacts on their trust and confidence.

4.6.5. 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?

The overall majority of respondents confirmed that there is a need to address liability issues for IoT services at EU level in order to ensure the roll out of these services and the free flow of data. On the one hand, businesses and business association are divided on this question, as half of the respondents in this category do not think that addressing liability issues at EU level is needed for the roll out of IoT and to ensure the free flow of data, while the other half support regulation at EU level. On the other hand, more than three fifths of individual users and associations representing customers and civil society expressed a view in favour of EU regulation.

4.7. Open service platforms

It is widely agreed that open service platforms have socio-economic and innovation advantages over closed service platforms. Some businesses replied that they need further clarification about the term 'open service platform'. Nevertheless, the majority of respondents agreed with its benefits. Open service platforms are more likely to be interoperable, promote innovation, enhance competition and create open innovation ecosystems. They improve equality and fairness within society, as well as trust and confidence between participants. Respondents tend to agree that no regulation should ever impede openness, and that regulatory or policy initiatives should be oriented towards assuring transparency, privacy and standardisation in order to ensure the advantages of open service platforms. Respondents also expressed doubts whether targeted policy initiatives can accelerate open service platforms; however, support for the development and take-up of open service platforms should be increased.

4.8. Personal data management systems

A majority of respondents across all groups are in favour of the promotion of technical innovations, such as personal data management systems.

A large majority of respondents (9 out of every 10) are in favour of a personal data management system, however only a small number of businesses (including online platforms) and business associations replied to this question, in comparison to other types of respondents. A large majority of respondents were individuals or associations representing consumers who are favourable towards initiatives at EU level supporting personal data management systems.

4.9. European Cloud Initiative

4.9.1. Key elements for ensuring trust in the use of cloud computing services by European businesses and citizens

More than two thirds of the businesses, citizens, research and think tanks who responded to this question consider that reducing regulatory differences between Member States is a key element for ensuring trust in the use of cloud computing services by European businesses and citizens. More than a half of the SMEs also indicated this as a key element.

A vast majority of all respondents groups (around three fifths of business respondents, SMEs, citizens and around four fifths of the research and think tanks and public

authorities) consider that investment by the European private sector in secure, reliable and high quality cloud infrastructures is important to ensure trust by users.

Around two thirds of the individual citizens and the research and think tanks and around half of the businesses and SMEs considered standards, certification schemes, quality labels or seals as a key element to ensure trust.

Half of the businesses and research and think tanks consider use of the cloud by the public sector as a key element to ensure trust by users, followed by SMEs (a few more than a third) and then citizens (around a quarter).

The majority of public authorities that replied to this question indicated that reducing regulatory differences between Member States was a key element to ensure trust by users, whereas one third indicated that standardisation and the use of the cloud by the public institutions was a central element.

4.9.2. Transparency of the cloud services on the security and protection of users' data and the fair and balanced allocation of legal and technical risks in existing contractual practices

Overall, respondents (from all respondent groups) believe that cloud service providers are not sufficiently transparent on the security and protection of users' data. A large majority of individual citizens, as well as associations representing consumers are among those who confirmed this lack of transparency. At the same time, a small majority of business respondents (cloud service providers) are of the view that cloud service providers are sufficiently transparent on the security and users' data with regard to the services that they provide. They are also of the view that users are sufficiently protected by existing legislation (such as the Directive on Unfair Terms in consumer contracts and the Data Protection Directive 95/46 and the upcoming GDPR); therefore, there is no need for regulatory intervention.

Responses shows that users of cloud services, including SME users, have a contrary opinion and consider that cloud service providers are not sufficiently transparent on legal and technical risks for the users and that security and protection of users' data are poorly explained by cloud service providers.

Businesses and individual citizens raised the point that negotiations between providers and users are unbalanced. Some indicated that cloud services are often provided on a "*as is*" basis, shifting the legal and technical risks onto the users. Some respondents indicated that there is also an imbalance between the users (namely big companies, SMEs and individual users) in terms of bargaining power when contracting with cloud services providers.

Respondents of all groups believe that cloud services providers should follow the principles of data protection by design, i.e. who has access to the data (data flow in transit, explicit consent, law enforcement access requests, subcontractors), and data jurisdiction, e.g. data storage location and company ownership. Respondents feel that cloud service providers should provide information on data location, data processing and transfer, access rights, right to modify and delete data, retention of data, technical security measures, encryption techniques, corruption of data, security breach and incident management process, third party access to data and law enforcement access requests.

Many individual users found the terms of use of cloud services unclear, complicated and too long. Some of them indicated that they don't even read contractual terms. They indicated that terms of use of cloud services lack transparency as to their user rights, liability, transfer of data to third party, security breach, and data storage.

4.9.3. The benefits of interoperability (cloud computing services interacting with each other) and of data portability between different providers of cloud services (including at European level)

Almost half of the respondents consider that ensuring interoperability and guaranteeing portability would lead to economic benefits. Nearly a third of respondents are of the view that ensuring interoperability and guaranteeing portability could improve trust. The remaining respondents had differing views where some commented that it is not necessary to regulate these topics, and others suggested that portability could stimulate or stifle competition in the market. This perspective stemmed from the consideration for moving of data for business users or for the right to portability for individual data subjects.

Moreover, some businesses (including business associations and online platforms) emphasised that portability and interoperability should not be a general or mandatory obligation for all providers but a competitive differentiator that could reduce or revise competition dysfunctions. Business respondents also expressed their view that interoperability should remain businesses' own decision.

4.9.4. Contractual practices encountered in relation to cloud based services which could hamper the uptake of cloud based services

The majority of respondents raised the point that the contractual terms and conditions are non-negotiable for individual consumers. Many businesses and SMEs indicated that they often encounter difficulties in negotiating terms and conditions for cloud services. Some providers explained that for business to consumer (B2C) contracts, they can't afford to negotiate with each user and to adjust their terms for each of them due to the size of their user-base, the necessity for cloud services to operate at scale and to be standardised and the need for cloud providers to remain competitive in the market, particularly when services are provided to a large number of users without charging fee.

The majority of the respondents encountered limitations as regards to the possibility of switching between cloud service providers. Respondents listed technical constraints in general, and more particularly data recovery, moving data, interoperability between systems and applications, incompatibility of some functionality, different data formats depending on services, lack of industry standards, among the elements that affect users' decision to switch between cloud providers or that make such a possibility costly. Some respondents highlighted that the lack of contractual provision on these topics created uncertainty.

The majority of the respondents encountered the contractual possibility for the supplier to unilaterally modify the cloud service. Some respondents indicated that cloud service providers need flexibility to update and improve their standardised services and to address new demands. Some respondents indicated that the possibility for providers to unilaterally modify cloud services reflects the imbalance of powers between the users and the providers in cloud contracts.

The majority of the respondents encountered limitations of the supplier's liability for malfunctioning cloud services (including depriving the user of remedies). Based on the responses received, we can however not conclude what the limitations most encountered by individual users or business users are.

4.9.5. On model contracts for cloud service providers as a useful tool for building trust in cloud services

The majority of the respondents in all groups (i.e. businesses and trade associations, SMEs, citizens and consumers associations, public authorities and research and think tanks) are of the view that model contracts would be a useful tool for building trust in cloud services. SMEs are nevertheless a bit more divided on the question as less than half answered that such model contracts would not be useful.

While more than two thirds of SMEs and a majority of businesses and trade associations indicated that their answer would not differ for B2C and for B2B cloud contracts, around half of the citizens and associations representing consumers as well as research and think tanks indicated that their answer would differ. A vast majority of public authorities would differentiate their answer for consumer contracts and for commercial cloud contracts.

Although the majority of respondents are in favour of self-regulation rather than regulation, the responses received do not allow the identification of trends for preferred alternative approaches other than model contracts in regards to both B2C and B2B.

4.9.6. The main benefits of a specific European Open Science Cloud which would facilitate access and make publicly funded research data re-useable

A vast majority of the overall respondents (four fifths) answered that the European Open Science Cloud would make science more efficient by better sharing resources at a national and international level. More than two thirds answered that it would create economic benefits through enabling better access to data held by economic operators. Around two thirds answered that it would make science more reliable by ensuring better quality assurance of the data, or more efficient, by leading to faster scientific discoveries and insights. Half answered that the European Open Science Cloud would make science more responsive and enable it to quickly tackle societal challenges.

About a fifth of the respondents see other benefits. The main answers could be summarised as follows:

- To complement open access and open data, the institutions should also reward openness in science, because the "publish or perish" stance taken by many research organisations, funding agencies and hiring boards does not encourage openness and collaboration.

- The private sector expresses some concerns that the commercial value of project results can be damaged if all data needs to be disclosed.

- A vast majority of the respondents from the Research and think tanks group and from public authorities replied that the European Open Science Cloud would have all the benefits mentioned above (i.e. make science more efficient by better sharing resources at a national and international level; create economic benefits through enabling better access to data held by economic operators; make science more

reliable by ensuring better quality assurance of the data, or more efficient, by leading to faster scientific discoveries and insights, and; make science more responsive and enable it to quickly tackle societal challenges). The main trend in the businesses and trade associations group, including SMEs, relates to creating economic benefits through enabling better access to data held by economic operators.

4.9.7. General comments and ideas regarding data and cloud computing

Many respondents outlined that a distinction must be made between cloud services offered to consumers and cloud services offered to businesses and referred to the existing EU legislation relating to consumer protection and the protection of personal data.

Many respondents from the business group raised the importance of the freedom of contracts in the B2B context and the flexibility needed by companies to explore new technologies and business models. Many of the business respondents believe that policymakers should refrain from preliminary regulatory actions as the data market is still in its early stage. Some of them explicitly warned against any action prescribing, dictating or promoting a specific business model in order not to stifle innovation. A few respondents indicated that cloud service providers are not just competing on pricing and that security, accountability and transparency are competitive differentiator as well. Some business respondents stressed the importance of market dynamics. They explained that as cloud is based on economies of scale, big cloud providers have strong competitive leverage compared to new entrants to the market. They encouraged the involvement of EU small cloud providers in any EU self-regulatory initiative as these providers have little time and resources to allocate to define their own internal policy, tools and processes. Finally, other business respondents warned specifically against certification schemes for cloud services that would be adopted at national level as this could lead to fragmentation and create data localisation requirements.

Many consumers raised concerns about the protection of their data when it is in the cloud. Consumers indicated that it is essential that their data is kept safe and private and that they would like to know where the data is located, who has access to it and whether third parties can access to their data based on national law enforcement. Many respondents from the consumer group stressed that technology evolves rapidly and that regulation risks hindering innovation.

Some respondents from the research and think tanks group also commented that regulation could slow down innovation.

Some respondents also pointed out that data security is not improved because data is stored locally and that localisation restrictions could not only increase the cost for users but could also limit their access to leading technologies.

CONCLUSIONS

The majority of stakeholders who responded to the consultation believe that data location restrictions may be a barrier to the development of the data economy in the EU. The consultation and stakeholder meetings confirm the need to take action to tackle legal and technical restrictions on the free movement and location of data, as envisaged by the DSM Strategy.

The results also indicate that policy initiatives are needed to ensure a more consistent application of rules, in particular as regards data protection, as well as to provide a clear and consistent framework for liability in data markets and IoT. There is also a need to look into and provide guidance on other issues such as data access and "ownership", usage and transfer. Based on specific use cases and where justified, mechanisms for enabling appropriate access and use of data adapted to a specific sector needs should be further investigated.

These findings will input directly to the impact assessment and draft initiative being prepared on the Free Flow of Data.

The stakeholders confirmed that the European Open Science Cloud would allow research to have a greater impact and make science more efficient by better sharing of resources at national and international level. The concerns expressed by respondents regarding the need for open research data and the possible benefits of an open science cloud will therefore be addressed in the Communication on the European Cloud Initiative, as part of the Digitising European industry package of the DSM.

These findings have been used in framing the European Cloud initiative to be adopted by the Commission in the coming days.