Annex to the Synopsis report

Detailed analysis of the public online consultation results on 'Building a European Data Economy'

Introduction

Context of the public consultation and purpose of this document

The public consultation on 'Building a European Data Economy' contributes to shaping the future policy agenda on the European data economy. The consultation took place from 10 January to 26 April 2017, and constituted part of a broader consultation process launched with the adoption of the Communication on Building a European Data Economy (COM(2017)9) and its accompanying Staff Working Document (SWD(2017)2).

The objective of the consultation was to collect information on:

- whether and how local or national data localisation restrictions inhibit the free flow of data in Europe;
- whether and to what extent digital non-personal machine-generated data is traded and exchanged;
- the nature and magnitude of any barriers to accessing such data;
- ways of tackling those barriers;
- emerging challenges relating to liability in the areas of the Internet of Things and robotics;
- practices and issues relating to data portability, interoperability and standards.

This annex to the Synopsis report analyses the replies to the questionnaire of the online public consultation in greater depth. The document is structured following the different sections and sub-parts of the questionnaire itself. The analysis also covers the position papers that respondents could attach at the end of their replies.

The conclusions of this consultation action serve as a basis for the synopsis report, alongside the conclusions of other consultation actions such as workshops. The synopsis report, of which this document is an annex, will cover the entire consultation process of the 'Building a European Data Economy' initiative.

Overview of respondents

The targeted respondents for this consultation were businesses of all sizes and sectors, including specifically manufacturers and users of connected devices, operators and users of online platforms, data brokers and businesses commercialising data-based products and services. Public authorities, non-governmental organisations, researchers, research organisations and consumers were also invited to contribute.

The online survey received a total of 380 responses, including 332 responses from businesses/organisations, 6 responses from self-employed individuals, and 42 responses from citizens. The 4 top participating countries were Italy, Germany, France and Spain. 28 % of the businesses/organisations that responded

operate in Belgium (including a lot of Brussels-based organisations such as European associations). The following 6 countries were Germany, France, the UK, Spain, the Netherlands and Italy.

The 'businesses/organisations' category of respondents includes organisations from both the private and public sector. Regarding the participation of the public sector in the public online consultation, 14 % of businesses/organisations indicate they belong to it, operating in Lithuania, Finland, Portugal, the Netherlands, Denmark, Sweden and others (11 countries were counted in total). Several Member States (Ministries and government bodies) communicated their contributions to this debate via different channels (e.g. functional mailbox) which will be analysed in the synopsis report.

Within the category 'self-employed individuals and businesses/organisations', the respondent category that constituted the vast majority of total respondents to the questionnaire, 22 % of respondents replied on behalf of a small or medium-sized enterprise (SME). From the same two categories of respondents, one can see that a third of them operate in IT services, which include applications and software developers, while 25 % indicated that they operate in the automotive and transport sector, pointing to this sector's strong interest in and commitment to discussing data access and liability issues.

Citizens were slightly more active in responding to the sections addressing 'data localisation restrictions', 'access and transfer' and 'portability' than those addressing 'liability' and 'interoperability and standards'.

Localisation of data for storage and/or processing purposes (free flow of data)

The objective of this first section of substantive questions was to obtain insights into the existence of data localisation restrictions and their economic impact on stakeholders.

As stated by the Commission in the Communication 'Building a European Data Economy' of 10 January 2017, data localisation restrictions relate to requirements imposed by public authorities on the location of data for storage or processing purposes. Data localisation restrictions can apply to a wide range of different types of data, including industrial and machine-generated data. They exist in different forms, from legal acts adopted by Member States to administrative rules and practices. Some of the data localisation restrictions will be addressed by the General Data Protection Regulation (GDPR), but that Regulation is limited to localisation restrictions for data protection reasons and only covers personal data. As the data economy is currently expanding, the use of non-personal data, e.g. in a business-to-business (B2B) context, is expected to become more important. The input provided by this section of the public consultation can help to determine how future EU policies could be shaped.

Private businesses and associations have been most active in responding to the questions in this section.

Examining stakeholder perspectives on data localisation restrictions

Some 303 out of 318 total respondents in this section replied to the question **whether a participant knows about legislation or administrative rules or guidelines (including those adopted in the context of public procurement) requiring the storage or processing of data in a certain Member State**. Of those respondents, about 67 % indicated that they know of such restrictions and roughly 33 % are not aware of any. Further analysis shows that businesses/organisations are more aware of such restrictions than individuals or self-employed respondents are.

When asked **what type of restriction(s) this concerns**, 196 respondents highlighted 'legislative requirements' (this was mentioned 174 times, so only 11 % of respondents did not select at least this option). 'Administrative rules' and 'guidelines' followed, with 91 mentions and 88 mentions respectively. When combined, administrative rules and guidelines were mentioned about the same number of times as legislative requirements.

To the question **which type of data this legislation or these guidelines concern**, 195 respondents answered by selecting one or more categories. The most frequently given category was 'personal data for reasons other than the protection of natural persons' (142 times), followed by 'business data in private hands' (133 times) and 'non-personal data publicly held' (87 times).

Of the 197 participants who responded to the question **whether they have to comply with the localisation restrictions** over 80 % stated that they/their organisations need to comply with these requirements against 11 % that indicated they do not to have to comply. 127 respondents took advantage of the possibility to qualify their answer. They identified restrictions, in either specific or general terms. The specific references point to both Member State legislation and sectoral guidelines, in the following proportion: roughly two out of three pointed to legislation, while the remainder pointed to guidelines. In some cases, different answers centred around the same restrictions. Finally, two larger corporations made reference to the existence of data localisation restrictions in the form of public procurement requirements. One of them mentioned that in some cases, it is unlawful to publicly communicate about these public procurement requirements. Only 10 respondents did not know whether the rules applied to them. Some stated that legal assessments are currently ongoing.

Examining the impact of data localisation restrictions

In the next questions, we will concentrate on potential impacts of data localisation restrictions on respondents.

To the first general question on **what these impacts are**, 193 of 318 respondents gave a reply. The impact that was most frequently mentioned across all participants was 'costs' (130 times). The second most frequent answer was that of 'launching a new product or service' (118 times), followed by 'entering a new market' (95 times) and 'providing services to private entities' (81 times). Other impacts such as 'providing services to public entities' or 'conducting research' received lower scores. Only 2.6 % (16 respondents) saw no impact of data localisation restrictions.

Some 35 respondents described the impacts in a qualitative answer. Among the impacts is a statistical overrepresentation of IT businesses when compared with the total group of respondents, in particular of cloud service providers (CSPs). In the majority of answers, they pointed to the impact of delivering services to private entities. CSPs present the argument that data localisation restrictions undermine the cloud business model, sometimes preventing cloud providers from accessing markets where they do not have a datacentre, and in other cases preventing cloud users from using services across borders within the EU. Some respondents focused on the impact in terms of higher costs, mainly when it comes to higher costs passed on to consumers because of the inefficient allocation of datacentres.

Respondents were asked to give **an appreciation to the nature of the impacts** as 'high', 'medium' or 'small'. This was specified per impact category used above. As this question yielded a large number of results, it is best to present them in the form of a table (see below).

Table — Impact of measures (high, medium, low)

What is the impact (if any) of such a measure, notably on your business or organisation?: Impact on (you) providing a service to private entities	High	Medium	Small	Total
Frequency	55	19	5	79
Percent	69.62	24.05	6.33	100
What is the impact (if any) of such a measure, notably on your business or organisation?: Impact on (you) providing a service to public entities, e.g. following public procurement	**High**	**Medium**	**Small**	**Total**
Frequency	40	15	9	64
Percent	62.5	23.44	14.06	100
What is the impact (if any) of such a measure, notably on your business or organisation?: Impact on costs	**High**	**Medium**	**Small**	**Total**
Frequency	73	37	14	124
Percent	58.87	29.84	11.29	100
What is the impact (if any) of such a measure, notably on your business or organisation?: Impact on entering a new market	**High**	**Medium**	**Small**	**Total**
Frequency	68	17	7	92
Percent	73.91	18.48	7.61	100
What is the impact (if any) of such a measure, notably on your business or organisation?: Impact on launching a new product or service	**High**	**Medium**	**Small**	**Total**
Frequency	82	21	10	113
Percent	72.57	18.58	8.85	100
What is the impact (if any) of such a measure, notably on your business or organisation?: Impact on (your) ability to carry out scientific research projects/studies	**High**	**Medium**	**Small**	**Total**
Frequency	22	17	5	44

Percent	50	38.64	11.36	100

It can be concluded that with all impact categories, a high impact level received more votes than a medium impact level, which in turn received more votes than the low impact level. Particularly for 'launching new products and services', 'costs' and 'entering a new market', respondents seemed convinced of the high level of impact.

There were also 32 qualitative responses to this question. As the results of the multiple choice question show, most respondents identified administrative costs in their answers (22 times). Another category of cost mentioned frequently is 'duplicating resources in different Member States' (19 times). 12.5 % of respondents specifically mention the detrimental effects of these costs for start-ups and SMEs. The answers explained that localisation restrictions make it harder for them to compete with incumbents because of increased costs due to the duplication of resources in different Member States.

Regarding impacts in terms of costs, the consultation included several further questions to retrieve information on the specific costs incurred. Participants were asked about administrative costs, costs regarding the storage of multiple copies and costs regarding the deployment of multiple servers:

Table — Impact on administrative costs

	Frequency	Percent
High	65	56.52
Medium	39	33.91
Small	11	9.57
Total	115	100

There were not many participants who could estimate the administrative costs, so this section was primarily used to give impressions of cost categories or further explanations. Such cost categories included the areas in which additional manpower was needed and compliance costs to meet local requirements.

The estimates given ranged from EUR 5 000 to 100 000 per year to EUR 1 million to EUR 50 million a year annually for administration and potential higher costs on failing to be compliant, for audits, breaches. Costs will be higher for businesses with more data and for businesses with more localisation needs, so there are considerable uncertainties associated with these estimates.

Table — Impact on costs from the storage of multiple copies

Answer option	Frequency	Percent
High	54	67.5
Medium	18	22.5
Small	8	10
Total	80	100

Although there were not many replies on this question in general, many respondents stated that the costs depend on the number of copies, the data volumes and data types (e.g. sensitive personal data) as well as on residency (localisation). Other respondents stated that creating more backups would introduce more costs.

Table — Impact on costs from multiple servers

	Frequency	Percent
High	48	52.17
Medium	41	44.57
Small	3	3.26
Total	92	100

One participant explained that most clients of companies offering server space would be in the retail and wholesale sector and qualify as SMEs. They would not have their own servers, but use cloud and other services provided by third parties. Multiple servers could therefore induce significant cost in deploying a global software as a service (SaaS) offering.

Regarding impacts in terms of costs, the consultation also asked whether these are **recurrent or one-off**. A large majority indicated that the costs are recurring rather than one-off: 95.6 % (of 91 respondents) concerning the use of multiple servers and 88.6 % (of 114 respondents) concerning administrative costs.

Removing data localisation restrictions?

In the next section, respondents were asked whether they see the need for removing data localisation restrictions. For their answers, see the table below.

Table — Answers to the question: 'In your opinion, should data localisation restrictions be removed within the EU?'

	Frequency	Percentage
Yes	185	61.9
No	55	18.4
I don't know	59	19.7
Total	299	100.0

The following question addresses the possible justifications for keeping data localisation restrictions.

Table — Justification for keeping data localisation restrictions

	Frequency	Percentage
Public security	176	39.6
Law enforcement needs	101	22.7
Public policy (such as immediate availability of data for supervisory authorities)	71	16.0
Other (such as a need to control or audit sub-contractors)	63	14.2
Public health	34	7.6
Total	445	100.0

Benefits of taking away data localisation restrictions

In terms of benefits of taking away data localisation restrictions, the consultation results confirm the picture that we have seen above regarding negative impacts of these restrictions. After the respondents were asked about **the benefits of a removal of localisation restrictions**, they mainly referred to the disappearance of the same problems identified in the 'impacts section' above, with cost reductions leading the list (with 45.28 % of respondents expecting cost reductions).

When asked to **quantify these benefits** in written responses, this yielded no exact quantifications. However, 36 respondents replied, providing different examples of possible cost reductions. Start-ups and SMEs were mentioned multiple times, in which cases it was stated that taking away localisation measures would reduce the cost of setting up a business in the EU, which is currently at EUR 300 and 3 days. An obligation to set up data storage in different countries would drive these costs above an acceptable level and eliminate benefits of digital technologies, as emphasised by respondents. An association of start-up companies stated that small companies act rationally when entering new

markets. If scaling across Europe is more expensive than scaling globally, start-ups will continue moving to other regions of the world to scale before they enter European markets. This view was repeated several times by other respondents.

Another example relates to the **diverging market characteristics** of data services in Europe. One respondent mentioned that a server for hosting health data in Germany costs EUR 3 000 per year, while this costs EUR 13 000 in France. The respondent states that taking away data localisation restrictions would drive down price levels and take away market distortions as a result of competition. Other market-related arguments mentioned were that it would expand the scope of targetable market, reduce red tape, complexity and time. Moreover, as start-ups are dependent on competitive cloud services, taking away localisation restrictions would increase their competitiveness. This would make it possible to go faster to market, to improve on the innovation pace and support scalability for start-ups and efficiencies.

One participant mentioned an asymmetric impact for companies with more data and for businesses with more localisation needs:

- Restricted access to data from abroad would put entrants on an unequal footing with national operators (for example in the case of railway transportation services).
- When start-ups have to store company data in several countries it becomes a major detriment to scaling up within the EU single market.

Yet another question addressed **the benefits in terms of security gains**. Among the 24 respondents to an open question on this topic were many IT companies, some specialised in cybersecurity. They repeated the argument that taking away data localisation measures would benefit data security, as it would allow transnationally operating CSPs to carry out safety updates across borders at the same time for all their users in the EU. They also mentioned that cyber incident detection should happen on a permanent, 'follow the sun' basis, meaning a high dependency on sharing information across geographies in a timely manner.

A final question addressing the benefits of taking away data localisation restrictions focused on the benefits in **terms of expanding sales to third-country markets**. Participants mentioned that taking away data localisation restrictions would foster new, cross-border cooperation, i.e. in health or education. Participants also cited easier upscaling of new business models based upon machine learning, AI and other technologies and methods. Yet another commonly mentioned element in the 23 answers to this question was the signal that the EU could give to the global community by means of a free flow of data principle. Conversely, some respondents fear a vicious cycle if the EU does *not* take away data localisation restrictions. It might incentivise other countries to put in place such restrictions as well.

Examining the current state of play of intra-EU data flows

This section briefly explores the state of play of intra-EU data flow, with the objective of investigating to what degree the respondents that answered are already **engaged in storing or processing data in multiple locations in the EU**. To the general question whether respondents are indeed already active in such cross-border activities, 54.3 % answered yes (278 of the 318 respondents that participated in this question). Analysing the outcomes on a sector-by-sector basis, it is significant that in financial services, 88.9 % of the respondents store and process data in multiple locations in the EU. In the case of the

public sector, the reverse is shown: only 15.8 % store or process data in multiple Member States. IT businesses and the manufacturing industry are in line with the overall percentages.

Some 39 respondents (all storing and processing data in multiple locations within the EU) explained their choice in a written answer. They mainly pointed to operational reasons, although the nature of these operational reasons differed. Examples are the cross-border character of their activities, the location of subsidiary companies and the satisfaction of consumer expectations for proximity. A second category of reasons concerned business continuity and security. A third and final category was data localisation restrictions in other Member States, which incentivises organisations to store their data in those countries instead of e.g. in a central depository. This last answer category was mostly given by business users of cloud solutions.

Those respondents that indicated that they do *not* process or store their data in multiple locations were also asked for their reasons behind this choice. Most participants stated that there was no need to store data in more than one location (because they have no operations in other countries), there were financing constraints, they do not use cloud services completely and/or they made promises to clients to keep data within borders. A particular argument standing out in this regard was the reference to the critical/confidential nature of the data as a reason for not storing or processing it in multiple locations (see table below).

Table — What is the importance of critical/confidential nature of the data as a reason for not storing or processing your data in multiple locations within the EU?

	Frequency	Percentage
High	21	65.6
Medium	10	31.3
Small	1	3.1
Total	32	100.0

Another question in this section is **whether customers have demanded that their data is processed or stored locally.** The answers to this question were dispersed. 40 % of total respondents indicated that they did not know or gave no answer. Roughly 30 % said yes and the other 30 % said no. For that reason, the answers to this question do not provide a clear picture. This changes when taking a sector-specific approach. Among IT-sector respondents, 60 % indicated that their customers have indeed demanded local storage. For financial sector respondents, this percentage was only 10 %. Hence, it may be inferred that it is predominantly IT businesses (e.g. CSPs) which receive demand for local storage.

The question on the **reasons customers have to demand local storage** confirms this insight. Although a small number of respondents answered it (87 respondents), there is a clear distinction between IT respondents (of which 60 % answered the question) and all other respondents (only 10 % answering the question). The reason which was most frequently mentioned overall was ‘an assumption/perception

that there is a local legal or administrative requirement to do so'. However, if the IT sector is not taken into account in the statistical analysis, this answer suddenly becomes the least mentioned.

Another reason that respondents identified for demanding local storage/processing was a lack of familiarity with EU rules. Participants were asked to describe these reasons in written answers, with a focus on familiarity of customers. Respondents mentioned several aspects in an approximately descending order of importance (according to the frequency of mentioning):

- need to analyse data locally;
- concerns about data security;
- belief that there are localisation mandates, even if there are none and no resources to verify whether there are such requirements/mandates;
- technical reasons (latency);
- cultural concern about storing data outside the jurisdiction;
- customers' belief that GDPR requires geo-fencing and data localisation for the purpose of data sovereignty;
- reasons for liability and place of jurisdiction (court), compliance risks;
- apprehensiveness of negative public reaction in the case of storing data abroad;
- critical nature of data (healthcare data);
- reservations about data being given up for law enforcement access in that very country, where it is stored;
- data localisation requirements put forward by certain Member States in public procurement;
- confusion about what laws of IT security and data protection would apply.

Examining possible ways forward

The final question on data localisation restrictions is about **what kind of action at EU level stakeholders consider appropriate to address the restrictions**. 289 respondents participated in the multiple choice question, of which the outcome was that 'a legislative instrument' seems the most appropriate action (151 times), followed by 'guidance on data storage/processing within the EU' (137 times) and 'increasing the transparency of restrictions' (128 times). 'Other' options received a significantly lower amount of selections (55 times).

Analysis of the open question on the same topic (answered by 47 respondents) shows that the answer that occurs most frequently is a **combination** of a **legislative instrument** and **increasing the transparency of existing restrictions** (14 times). The respondents' argument behind the call for a legislative instrument is that this provides clarity and legal certainty by establishing a general principle of the free movement of data. Apart from this, respondents believe that a regulation sends the strongest signal to the international community, showing that the EU takes leadership on the free movement of data. As there are currently already data localisation restrictions in place, a number of these respondents also called for transparency on the approach to those existing restrictions. Some

stakeholders would prioritise increasing transparency as they believe it would cost too much time to wait for a legislative instrument to come into force. Respondents that called for a regulation were mostly from an IT background, with large tech giants and CSPs within their ranks.

However, not all respondents favour a regulation. A second category asked for an approach using the already existing regulatory framework. In particular, they favour the removal of unjustified data localisation restrictions by extending the notification procedures already established by EU law under the E-Commerce Directive, the Services Directive or the Transparency Directive. A sectoral analysis shows that participants who answered along these lines (5 responses) are all from the telecom sector, except for a contribution by an association for businesses involved in intellectual property and patents.

A third category of respondents (5 responses) called for further analysis and assessment to be conducted by the Commission before making a choice about the most appropriate instrument.

Conclusion

A majority of respondents know data localisation restrictions. Roughly one third of the respondents qualified this with descriptive input. 80 % of respondents stated that they/their organisations have to comply with these restrictions.

There is broad consensus among stakeholders about the existence of impacts of data localisation requirements, with only 2.6 % of respondents indicating that they do not see any impact. For all possible categories of impacts that were tested, most respondents indicated that they saw high impacts, followed by medium impacts. A relatively small number of respondents identified low impacts. As regards specific categories, the highest impacts of data localisation were identified to be on costs, on launching a new product or service and on entering new markets. The types of costs incurred were mostly administrative costs and costs relating to the duplication of resources in different Member States. A large majority of respondents pointed to the recurrent nature of these costs. Some respondents mentioned the specifically detrimental effects of costs related to the duplication of resources for start-ups and SMEs, who will be unable to compete with incumbents on these terms.

When stakeholders were asked if they believed that data localisation restrictions should be removed, just over half answered yes. When limiting the analysis to SMEs, roughly 60 % answered yes, with a small minority arguing for the opposite. When asked for justifications to keep localisation restrictions, respondents mentioned public security, law enforcement purposes, concerns about confidential data and the need to control their sub-contractors (e.g. sub-contractors offering data storage/processing services).

Stakeholders pointed to various benefits that could be derived from taking away data localisation restrictions that are in place. Firstly, and in line with the above, they pointed to cost reductions, specifically mentioning more favourable conditions for SMEs and start-ups to conduct business in Europe. They also mentioned that competition would drive out market distortion that is currently present (one respondent gave an example of highly divergent server prices in different Member States). Another benefit relates to data security, which would benefit from the free movement of data because of the possibility to perform cross-border safety updates at once among users of cross-border cloud

services. Finally, respondents believe that by taking away data localisation, the EU would send a strong signal to the international community, stimulating the free movement of data globally.

Little over half of the participating respondents are already active in storing and/or processing data in multiple locations in the EU. A sector-specific analysis shows that cross-border data processing and storage is much higher in financial services (88.9 %) and much lower in the public sector (15.8 %), whereas IT businesses and the manufacturing industry show figures similar to the overall proportion. When asked why respondents are processing and storing data in multiple Member States, general operational reasons were the most common answer. Some customers, predominantly of IT services like cloud computing, demand the local storage and processing of their data. This is mostly inspired by an assumption or perception that this is needed because of local legal requirements or administrative guidelines.

In terms of the most appropriate action to address the data localisation restrictions, a legislative instrument received the most support (151 times), followed by 'guidance on data storage/processing within the EU' (137 times) and 'increasing the transparency of restrictions' (128 times). 'Other' options received a significantly lower amount of selections (55 times). A number of respondents indicated that it would be appropriate to combine a legislative instrument with transparency on the already existing data localisation restrictions.

Access to and re-use of non-personal data

This section of the public online consultation aimed at finding out more about current business practice with respect to data sharing, separating the demand and the supply side and investigating any potential barriers that discourage companies from data sharing.

In line with the nature of the questions and the overall participation in this online consultation, the bulk of responses came from business or organisations.

Examining the demand side

With this set of questions, the public online consultation sought to obtain a better picture of the demand side of data sharing in terms of companies' dependency on data from external sources and their experiences in this respect.

Some 299 responses were received to the question on **dependency on external data sources**, 262 on behalf of business or organisations. 56.9 % declared that they depend to a significant extent on data resources that they acquire from others, while 43.1 % said that this was not the case.

In terms of **sources** currently used or relevant for future data usage, only 167 respondents provided an answer, 148 on behalf of business or organisations. Commercial or technical sources are used by 44.3 % of respondents, 25.1 % named public sources and 30.5 % replied 'other sources'. As results from the analysis of the free text field show, this appears to include data directly provided by individuals.

When asked about the **remuneration conditions** under which such data is accessed, 158 respondents selected one or several of the multiple answer options: 62 % indicated that they receive some of the data for

free; 57.6 % indicated that they receive some of the data against payment; 35.4 % said they provided a service in return and 22.7 % indicated another form of compensation.

When asked about **difficulties experienced when acquiring data from external sources**, 283 participants responded, 248 of which on behalf of business or organisations. 53 % of respondents declared that they had not experienced difficulties, whereas 47 % indicated that they had experienced difficulties (133 respondents). 129 respondents specified the **nature of such difficulties**. 26.9 % of all respondents to this question have experienced denial of access to data, 19.2 % have been exposed to terms and conditions that they considered unfair, 15.7 % have been asked to pay prohibitive prices and 11.3 % have seen a data licensing agreement being terminated in an unforeseen manner that did not allow them to adapt their business model. 21.2 % named other types of difficulties.

In terms of detailed comments, respondents from the automotive and transport sectors specified that car manufacturers in their view restricted access to in-vehicle data, by either not making the data available at all or only against prohibitive prices. Real-time data access was rarely available. The same actors, together with the association of automobile clubs, reiterated this position at the EC workshop on data and smart manufacturing held on 6 June 2017, while car manufacturers invoked issues such as safety, security and liability as reasons for keeping control over in-vehicle data. Respondents from the energy sector underlined that technical barriers may arise when systems are installed by others. Respondents from the insurance sector claimed that producers of devices and online platforms restricted data access.

The consultation then specifically asked whether respondents felt themselves to be in situations of **equal bargaining power**. 19.4 % of respondents believed that this was true 'to a great extent', 17.5 % said this was the case 'to some extent', 15.2 % felt that this was the case 'to a minor extent' and 29.3 % said that this was 'not at all' the case. 18.6 % did not voice an opinion.

Asked about whether they had been exposed to a situation of **abuse of dominant position** in such negotiations, 20.5 % said that in their view this had been 'often' the case, 14.7 % said this had been 'sometimes' the case, to 15.1 % it had 'rarely' occurred and to 23.6 % 'never'. 26.3 % did not voice an opinion.

The online consultation then sought to find out to what extent two areas of legislation, namely legislation regarding unfair contract terms or unfair commercial practices and competition law, were deemed adequate to address the issues identified.

With respect to **legislation regarding unfair contract terms or unfair commercial practices**, only 29.9 % of the 311 respondents in this section answered. 79 % of those respondents (31.5 % of all participants that answered questions in this section of the consultation) considered that such legislation did not address the problems experienced sufficiently, whereas 21 % (8.4 % of all participants) considered that it did.

Out of the 98 respondents who considered that current legislation did not sufficiently address the problems experienced, 38 considered the legal framework for ensuring fair commercial practices in B2B situations as such inadequate. 32 were of this opinion for the legal framework ensuring fair contract terms in B2B situations. 44 respondents named enforcement problems.

Some 39 respondents provided additional remarks through a free text field. At least a quarter of these respondents came from the automobile sector. In this sector many respondents pointed out that the legislation enabling access to data was insufficient or lacking. Some respondents mentioned Regulation

715/2007 (as amended), which contains rules on access to repair and maintenance information for vehicles but does not cover prediction and diagnosis. In general, some respondents underlined the monopolistic situation of some data holders and the lack of an adequate legal framework while others mainly pointed to the lack of effective enforcement.

When asked about the **effectiveness of competition law and its enforcement** in addressing potentially anti-competitive behaviour of companies holding or using data, 22.5 % agreed that it was effective 'to a great extent', 15.5 % thought this was 'to some extent' the case, 7.4 % said so to 'a minor extent' and 23.9 % considered that it was not effective. 30.6 % of respondents had no opinion on this question.

Even those respondents who agreed to some extent that competition law and its enforcement were effective nevertheless believed that competition law should evolve in order to adapt to the digital economy and to duly account for the reality of data-driven markets (network effects, self-learning algorithms, switching costs, etc.). Enforcement mechanisms should be applied in practice more actively and swiftly with regard to holders of large quantities of data, in light of the dynamic nature of data-driven markets. Up to now, data in their view had not been appropriately or systematically included in the assessment of potential abuses of a dominant position or when assessing mergers and acquisitions. There was allegedly a lack of broadly accepted methodologies and metrics to assess the economic value of data and to identify relevant markets where disruptive data-driven innovation cuts across market segments. These comments appeared regardless of the size or the sector of the given respondent.

Several respondents also pointed to the difficulties that the concept of 'data sharing' poses to competition law, which traditionally mainly focuses on products and services. SMEs stressed that consumers, new entrants and SMEs in general would need a better balanced protection vis-à-vis large data holders. Respondents also claimed that Europe had a viable interest in ensuring that its industry does not lose customer interfaces to the benefit of non-EU based tech giants. Operators in the automotive aftermarket in particular considered the current competition law to be insufficient and regretted the absence of regulation that would make the data collected by connected vehicles available to all. Telecom operators and trade unions proposed imposing an obligation on the largest data holders to license data usage to other companies operating in the same market, making sure that fair prices and conditions are applied ('obligation to license under FRAND terms', see infra). A legal professional deemed the creation of a new right in data ('data ownership right, see infra) as essential to make up for the shortcomings of current competition law. Concerns have also been raised about the inadequate considerations of consumers' data in mergers and acquisitions. Smaller companies active in the transport and energy services would welcome clearer rules on access to data held by transport and energy operators respectively.

Finally, we asked to what extent companies have entered into contracts in which data was defined as **trade secrets**.

About half the respondents (46 %) have entered into contracts in which certain data was defined as a trade secret. These respondents explained that the identification of trade secrets was done in relation to: licensing in/out data for further re-use (19 %); performing or buying data analysis services (18 %); sales/acquisitions of machines, tools or devices with embedded sensors (11 %); or in all these circumstances (12 %). Another 20 % of respondents referred to other contractual relationships in the context of providing consultancy, auditing, software-related or telematics services to customers or in the context of partnership/cooperation agreements.

Respondents provided, however, little insight into how the data in question was defined as a trade secret. Only 30 % of them replied to the question. The consideration of data as a trade secret often results from general contractual clauses (e.g. a general clause on intellectual property or a non-disclosure or non-use clause) assigning the data in the contract to a party. Only one respondent referred to national security as source of secrecy. A few respondents, on the other hand, claimed that these clauses are not really consensual but rather imposed by the data provider irrespective of whether the data could fall under the definition of trade secret in legislation. A few respondents provided examples of data which could be considered trade secrets: e.g. the process data collected for prescriptive analytics, which was regarded as competition-relevant know-how.

Respondents reported that the parties who more often claimed to hold data falling into the trade secrets category are: producers of sensor-equipped machines, tools and/or devices (20 %); data analysis service providers (16 %), data platforms gathering large datasets (14 %) and users of machines, tools and/or devices with embedded sensors (10 %). Other reported categories (18 %) were: data producers (e.g. transport companies), vehicle producers, customers, software companies or generally any party within the value chain.

Examining the supply side

With this set of questions, the public online consultation sought to better understand the supply side, in other words, the situation of current data holders.

Data holders were asked **to which extent they license data they hold to others**. Out of the 272 respondents to this part of the questionnaire, 237 respondents answered on behalf of a business or organisation. 57 (20.3 %) indicated that they make certain data available on the basis of an open licence (i.e. allowing many re-use options and free of charge, at least for non-commercial re-use of that data). From the analysis of the free text answer field, it turns out that an open data approach is particularly used for non-commercial re-use. 30 respondents (12.7 %) share some of their data with a wider range of players on the basis of a paying licence and 27 respondents (11.4 %) do so only within innovation environments, collaborating with companies on concrete protects. 44 (18.6 %) share data only with sub-contractors and 30 (12.7 %) only within the same economic group. 35.9 % indicated that they do not share any data or do so only to a minor extent.

Many holders of large amounts of data (e.g. telecoms) seem to favour either analysing data in-house or licensing data only to companies with whom they already have a close business relationship. Some mentioned a lack of standardised practice in this area and the use of customised licences depending on the project at hand, on a case-by-case basis.

Trade association bodies and other umbrella organisations underlined the highly diverse nature of the practices in the field. They mentioned that it would be difficult to identify any specific trends in that domain and that companies use various types of licences for different data or for specific data services only.

Utility companies (e.g. energy providers) indicated that the re-use of their data, along with other business activities in the sector, is often tightly regulated. This influences the choice of the licensing arrangements used. However, they also reported allowing open re-use of some of their data, for instance for non-commercial purposes.

Companies from the IT sector reported using a wide array of licensing arrangements, e.g. based on the commercial sensitivity and value of the data or the context in which the data will be used. This also includes open data licensing in some cases, but overall a negotiated and a case-by-case approach appears to be dominant.

When asked about the **motivations** of sharing or not sharing data, only half of respondents specified reasons: 28.7 % of respondents cited strategic business decisions, 17.3 % cited the fear of misappropriation of the data by others, 13.9 % mentioned legal uncertainty, 9.7 % said that they could not see any secondary usage for their data and 4.2 % said that they were unable to find the appropriate licensing conditions. 10.6 % cited 'other reasons'.

From the responses to the free text field, it emerges that some companies that make available some of the data they have to a wider range of economic operators as 'open data' (e.g. energy providers, railways) do so in order to encourage the development of new products and innovative services which are of interest to their customers.

Reasons for adopting bespoke licensing solutions cited were the requirement to adapt to a specific business model or cybersecurity threats. The commercial and reputational impact of any data transfer is another factor taken into account. Some respondents indicated that legal uncertainty with regard to the nature of data as an economic asset (e.g. tax treatment, liability in the case of a data breach, accounting rules, de-anonymisation) forced them to adopt very restrictive licensing practices or to abandon the sharing of data altogether.

The public online consultation also sought to better understand whether data holders feel that existing EU legislation **sufficiently protects investments made in data collection by sensors embedded in machines, tools or devices**.

Some 37.1 % of respondents believed that this is the case and only 16 % disagreed. 8.2 % indicated that current legal protection was limited to specific scenarios. 38.7 % of respondents said that they did not know.

In terms of **incentives to be given in order to encourage wider data sharing**, respondents were given the opportunity to make concrete suggestions.

No clear trend can be identified. While a number of respondents said that the Database Directive already provided sufficient incentives, others called for a clear regulatory framework on what data could be shared. Others stated that financial incentives would be important or at least ensure that the economic benefits outweigh the costs. Finally, some respondents underlined that an incentive would be reciprocity, namely being able to access data from other actors (mainly in the same ecosystem).

Very few participants (49 out of 237) responded to the question as to whether the intended use by the business partner has an influence on the **remuneration asked by the data holder**. 17 said that this influenced their decision to a 'major extent' (e.g. asking lower fees for non-commercial usage scenarios), while 15 said that this had only a 'minor' influence and 17 said that it did not influence the decision on the remuneration at all.

Similarly, very few respondents (45 out of 248) responded to the question **what types of data are being shared** and what types of data are not being shared. The only clear trend concerns data which is not shared. Personal data or data qualifying as business secrets are most frequently mentioned falling into this category.

Different examples of data that are being shared were mentioned; a small number of respondents (less than 5 for each example) each mentioned: scientific/research data, anonymised data on energy consumption, anonymised data on transport (e.g. timetables, lines tracing).

Finally, we asked companies whether they **introduced the value of at least some of their data holdings in the corporate balance sheet** — as recognition of its character as a corporate asset. This, however, turns out only rarely to be the case: 94.7 % of the 171 respondents who answered the question said that this was not the case. Only 9 respondents (5.3 %) said that they did.

Some 28.7 % of the respondents replied that they do not include their data as a business asset in their balance sheets as this was not required by the applicable accounting/financing reporting standards. 18.9 % expressed difficulty with regard to measuring the value of data. 9.2 % of respondents mentioned considerations of commercial strategy.

A small proportion of respondents explained their replies given to the previous questions in the free text field: in some jurisdictions accounting laws do not foresee the inclusion of data as one of the assets in corporate balance sheets. Others pointed to the fact that the company did not consider itself as the 'owner', but rather its customers. In some instances data was provided for free. Others considered that the value is not in the data, but rather depends on the services that build on top of it. Finally, some considered that once data appears in the corporate balance sheet it would also be subject to taxation.

Examining stakeholder views on possible ways forward

In this part of the public online consultation we asked participants to evaluate potential options for future development of the European data economy.

(i) Assessing the general objectives for the future EU framework of data access

Communication COM(2017) 9 'Building a European Data Economy' had set out a number of **general objectives for the future EU framework for data access**. The public online consultation sought to understand to what extent stakeholders agreed with those objectives.

Some 60.8 % of respondents (175 respondents) support the statement that data sharing should be enabled to a greater extent than it is today (stating that they agree 'to some' or 'to a great extent'). 15.7 % of respondents disagreed (48 respondents). The remainder of the respondents stayed neutral. Similarly, 67.7 % of respondents (194 respondents) supported the view that such data sharing should be facilitated and incentivised (stating that they agree to some or a great extent). 14.28 % disagreed (41 respondents). The remainder stayed neutral.

Some 65.4 % also believed that lock-in effects in the data market should be minimised, in particular for SMEs and start-ups. Only 8.6 % of respondents disagreed with this statement. The remainder stayed neutral.

On the other hand, a large majority also agreed with the statements that investments into data collection capabilities and data assets should be protected and that sensitive business data needed to be protected. 59.3 % agreed 'to some' or 'to a great extent' that investments need protection (16.1 % disagreed, the remainder stayed neutral). On the other hand, 78.6 % considered the need to protect sensitive and confidential business data ('to some extent' or 'to a great extent'), while only 10.5 % disagree (the remainder stayed neutral).

(ii) Assessing the possible ways forward

The Communication 'Building a European Data Economy' also presented a number of possible ways forward (described in more detail in the accompanying Staff Working Document SWD(2017)2). The public online consultation sought stakeholders' views on those possible ways forward and asked them to ascertain the likely impacts.

(a) Maintaining the status quo: Companies determine data sharing through contracts without any Commission intervention

The **first** possible way forward we asked about was essentially **keeping the status quo**, namely **leaving it to companies to determine re-use** of data collected by sensors embedded in machines, tools and/or devices **through contracts**.

Proponents and opponents to this question were exactly identical in numbers: out of the 297 respondents to this question 103 respondents (34.7 %) either agreed or disagreed with the statement that more data would become available for re-use if it was left to the parties to determine whether, how and under which conditions data should be shared. 59 respondents (19.9 %) said that this approach would at least 'sometimes' lead to more data being shared. 10.8 % of respondents did not know.

Looking at the 264 responses from businesses and on behalf of organisations only, 37.5 % of respondents fully agreed with the statement and 19.3 % respondents said that it would lead 'sometimes' to more data being shared. 33.0 % of business respondents, on the other hand, disagreed and 10.2 % said that they did not know.

The supporters of contractual arrangements argued that existing contractual mechanisms promote data-driven innovation (e.g. data brokerage). They claimed that only the freedom to contract can guarantee the flexibility needed to develop the data economy by taking into account all possible current and future business models and accommodating technological progress. This would exclude one-size-fits-all rules. In their opinion, contractual freedom is an incentive in itself (contrary to regulation). Also, business models only emerge at this stage. Such opinions were voiced in particular by trade organisations, companies from the manufacturing sector, IT providers and telecom operators. Some of the respondents qualified their support for contractual solutions by stating that an appropriate competition law framework should nevertheless be in place to prevent abuse and market misbalance.

Respondents who argued that contractual arrangements themselves would be insufficient (e.g. consumer associations, start-ups, public authorities, SMEs commercially re-using data) claimed that relying on contractual solutions only risks putting the manufacturer in a position that allows it to dominate or even monopolise the after-sales markets, e.g. by the provision of repair and maintenance services. The manufacturers could dictate data usage terms and thus limit competition. Stakeholders also claimed that if no clear principles protecting the weaker link in the data value chain are set at EU level, the benefits will not be fairly distributed across this value chain. Such respondents pleaded for a fair and flexible regime for access to and re-use of data collected by sensors embedded in machines, tools and/or devices.

This argument is most prevalent in the automotive and transport sector and, in general, in all situations where the market is characterised by the existence of a dominant economic actor (and data holder at the same time). In the case of the automotive after-sales markets in particular (including the automotive aftermarket and other services such as provision of insurances, satnav services), prolonging the current

situation (a *de facto* control of data by manufacturers) would likely to lead to restricted access to the data for all independent operators in the after-sales markets.

(b) The Commission issues a guidance document on how access, use and re-use of data should be addressed in contracts

The **second** possible way forward considered in the Communication COM(2017)9 was for the Commission to issue a **guidance document** on how access, use and re-use of data should be addressed in contracts (data usage licences) — based on existing legislation (in particular the Trade Secrets Protection Directive, copyright legislation and the Database Directive), essentially helping drafters of such contracts to better understand how existing legal rules should be read with respect to data sharing agreements.

Out of the 300 respondents, 30.7 % took the view that more data would become available if the Commission were to issue such guidance, 23.3 % believed that this would be 'sometimes' the case, whereas 29.7 % believed it would not have an impact. 16.3 % said they did not know.

The respondents that fully support guidance as a means to make more data available for re-use argued that it would address uncertainties and complexities, and foster awareness on possibilities to share data. This would be particularly useful to SMEs, new players in the data market, and to non-commercial operators (civil society). Some respondents specifically highlighted the need for guidelines on common standards and formats, and how differently personal and non-personal data should be treated.

Respondents disagreeing with the statement do so on two completely different grounds: one group considered contractual arrangements and/or general contractual laws sufficient to address data-sharing needs. Some respondents are in fact were concerned that any guidance may provide more confusion than clarity. On the other hand, another group of respondents disagreed with the statement because they considered it to be insufficient to encourage more economic players to share data. Those are the respondents that would favour harder options, for instance in the legal framework. It is not possible to deduce solid numerical information on the proportion of respondents that reacted negatively for this reason.

Some stakeholders took the view that sector-specific guidelines would be more useful than guidelines aiming to address data sharing across all sectors.

(c) The Commission supports the use of Application Programming Interfaces (APIs)

The **third** possible way forward considered in Communication COM(2017)9 was the use of **Application Programming Interfaces (APIs)** in order to enable data access and re-use.

Respondents largely agreed that a wider use of APIs would make more data available for re-use. 68.0 % of 284 respondents to this question fully agreed and 15.8 % said that this would be 'sometimes the case'. Only 5.3 % disagreed entirely (10.9 % of respondents chose the 'I don't know' option). Figures are largely the same if analysed by responses from business or on behalf of organisations.

Asked about specific measures the Commission could undertake to make more companies use APIs, 185 respondents replied to one or several of the multiple choice options: 108 respondents pleaded for technical guidance on how to design user-friendly APIs, 105 respondents said the Commission should promote knowledge about the benefits of APIs and 95 respondents could see benefits in introducing an API labelling

system (measuring e.g. the documentation, developer availability, access licence costs, etc.). 46 respondents saw 'other' ways to support the use of APIs by companies.

A number of respondents in the free text field remarked that the question is stating the obvious. APIs are only a channel for making data available and if such a channel was opened by companies, naturally some data would be shared. In this respect, APIs in themselves do not replace the underlying business decision by the company to make available data.

Respondents, including data holders, pointed to the widespread use of APIs. Some believe that it goes without saying that APIs are findable and well-documented, as otherwise there would be no point of making them available. Others highlighted the importance of making APIs secure so that the back-end systems are sufficiently protected against intrusion.

Some respondents feared the Commission would make APIs compulsory and argued that any such obligation should only be applied to the public sector.

(d) The Commission proposes a set of recommended standard contract terms

The **fourth** possible way forward considered in Communication COM(2017)9 was to draft a **set of recommended standard contract terms** in close collaboration with stakeholders.

Out of the 283 respondents to this question, 36.0 % agreed with the statement that more data would become available for re-use if such a set of recommended standard contract terms was to be drafted. 19.4 % believed that such recommended standard contract terms would at least 'sometimes' achieve that result, whereas 31.1 % disagreed with the statement. 13.4 % of respondents said that they did not know. Results were largely the same for businesses and on behalf of organisations. The workshop on data and smart manufacturing on 6 June 2017 presented a suggestion that invoices would also benefit from standardisation, as well as processes for data owner authorisation and authentication.

Arguments brought forward by those respondents that foresee a positive impact from recommended standard contract terms were: Trusted standard terms – if drafted in cooperation with stakeholders and then accompanied with communication actions – are likely to give an incentive to share data and develop new business models. They could provide important guidance and level the playing field by enhancing the bargaining power of the weaker party which may not have access to adequate a legal expertise (SMEs, consumers), and lower transaction costs. Some respondents emphasised that they would need to be well-crafted, using flexible, clear and simple terms.

Similar to the stakeholder reactions on possible Commission guidance, stakeholders that either oppose this way forward and/or do not expect a positive impact had two opposing positions: one group points to the freedom of contract, which should not be limited, and to the fact that the existing legal framework, including competition law rules, are working well. Restrictions of contractual freedom could diminish incentives to share data. This could therefore have a negative impact on competition and innovation. Also, a horizontal approach may be not detailed enough so as to cater for sector-specific requirements. Another group fears that big market players are unlikely to make use of such standard contract terms and therefore the impact would be limited. Consequently, the use of such standard contract terms would need to be monitored in some form by the Commission or another regulatory body. It is not possible to deduce solid numerical information on the proportion of respondents that reacted negatively for this reason.

Some stakeholders took the view that it was not possible to assess the possible impact on competition and innovation and that such assessment would depend on the concrete content and the actual use of the contract terms.

(e) The Commission adopts legislation laying down non-mandatory rules for B2B contracts

Under the **fifth** possible way forward considered in Communication COM(2017)9 **legislation would establish a set of (cross-sector or sector-specific) non-mandatory contract rules for B2B contracts**, possibly coupled with an unfairness control in B2B contractual relationships, for allocating rights to access, use and re-use data collected by sensors embedded in machines, tools and/or devices.

Some 24.5 % of the 282 respondents to this question believed that such a measure would make more data available for re-use, while 17.7 % said that this may 'sometimes' be the case. On the other hand, 41.1 % disagreed, while 16.7 % chose the 'I don't know' option. Figures were largely the same for responses from business and on behalf of organisations only.

As results from the analysis of the free text fields, respondents disagreeing with the statement that non-mandatory contractual rules for B2B situations would result in more data becoming available for re-use stressed the lack of evidence that there is a real problem which would justify the need for legislation. In their view the risk of unfair commercial practices was not new and was adequately dealt with by the current framework. They further considered that rules set in legislation would harm innovation and new business models and conflict with the freedom of contract. Also, such rules might lead to additional compliance costs.

Some stakeholders argued that they were unlikely to be adequate in practice as the contractual requirements with respect to data sharing vary widely between industry sectors and therefore a one-size-fits-all approach would not be appropriate. They feared that even if such legislation would only create non-binding rules which could be set aside by contract, such rules could risk turning into binding rules as a result of jurisprudence.

Respondents agreeing with the statement, on the other hand, argued that such rules could level the playing field against the background of asymmetries inside industry and help the weaker party, in particular SMEs with access to relevant data, notably by lowering transaction costs. They would ensure free competition and increase legal certainty. This would lead to new services and products. Combined with rules for the control of unfair terms, such legislation would in their view have positive impacts on data access. Some stakeholders go as far as calling for mandatory rules that could not be set aside by contract and systematic unfairness control.

A number of stakeholders point to the difficulty of laying down standard rules that are valid for every industry and sector. This was a challenging task, requiring detailed discussions with stakeholders.

Some stakeholders point to the difficulty of assessing the impacts of such measure, in particular as a result of the ambiguous nature of the concept of 'fairness'.

(f) Creation of a 'data ownership right'

Under the **sixth** set of ideas for possible ways forward the public online consultation asked for stakeholders' views with respect to three linked ideas for possible ways forward to **reinforce the legal position of the data**

holder in the form of some kind of 'data ownership right' that could take different forms and be allocated to different parties.

Under the first alternative idea on how such a 'right' would be defined, companies that hold data and protect the data through technical means against illicit misappropriation of such data by others would be given **civil law remedies against such misappropriation** (e.g. the right to seek injunctions, market exclusion, or to claim damages), in particular by third parties with whom the company has no contractual links. This would fall short of introducing full ownership rights (in the form of a *sui generis* intellectual property right).

Some 28.7 % of the 272 respondents said that such additional protection would lead to more data being shared for re-use and 17.6 % said that this would apply 'sometimes'. 27.6 % of respondents, on the other hand, did not agree with the statement, while 26.1 % chose the 'I don't know' option. Figures are largely the same for responses from business and on behalf of organisations only.

From the analysis of the replies to the free text field, it appears noteworthy that large data-holding companies are also divided on this question. In the written comments received, both support and opposition to additional civil law remedies were expressed.

Respondents were sceptical for completely different reasons:

Next to doubts about the feasibility to formulate a clear rule on who would benefit from such legislation, a significant number raised the issue that this may have a chilling effect on re-use of third party data as it increases the burden on the data supplier to demonstrate that such supply was lawful.

On the other hand, a considerable number of respondents believe that the existing legal framework is sufficient, i.e. the Trade Secrets Protection Directive, criminal law sanctions available in some countries, and the possibility to sue on contractual grounds. Others note that such civil law remedies would not be fast enough to address the needs of smaller companies in particular. Overall, technical protection mechanisms were considered to be sufficient.

The second, third and fourth alternative ideas on how such a 'right' would be defined have in common the creation of an '**exclusive right to license the use**' of the data collected by the sensors embedded in such machines, tools and/or devices. In other words, the ideas include the creation a sort of *sui generis* intellectual property right on data ('**data ownership right**'). Conceptually, such right would encompass the civil law remedies against misappropriation considered under the first alternative idea.

The options differ by the entity to which such a right should be allocated: under the **second** alternative idea it would be the manufacturer of the machine, tool or device ('companies active in the production and market commercialisation'). Under the **third** alternative idea, the right would be allocated *ab initio* to what the Communication 'Building a European Data Economy' referred to as the 'data producer' (the 'entities that operate sensor-equipped machines, tools or devices at their own economic risk'). Under the **fourth** alternative idea, such exclusive right to license would be allocated jointly to the manufacturer and the 'data producer'.

In a **comparative analysis**, it turns out that the two ideas under which a data ownership right is granted to either the manufacturer or the 'data producer' are viewed with the strongest scepticism. Scepticism is strongest for the idea of granting such a right to the manufacturer of a sensor-equipped machine, tool or device: 65.8 % of respondents took the view that such a measure would not have the effect of making more

data available for re-use, whereas only 8.6 % said that it would and 9.7 % said that it would 'sometimes' (15.8 % chose 'I don't know').

Some 51.8 % of respondents were sceptical that granting a 'data ownership' right to the producer would have positive effects on data sharing, whereas 12.3 % believed it would and 18.5 % took the view that this would be 'sometimes' the case (17.4 % chose the 'I don't know' option).

A shared 'ownership right', on the other hand, was seen more favourably: Only 27.4 % believed that it would not have beneficial effects on data sharing, whereas 33.6 % say that it would have beneficial effects and 23.5 % believed it would 'sometimes' have such beneficial effects (15.5 % opted for 'I don't know').

Responses to questions on all three ideas were largely the same when the analysis is concentrated on the business and organisations response only.

The idea of a joint ownership right gathered more positive reactions than the idea of merely introducing additional civil law remedies against misappropriation of data.

From the input received through the free text response field, it appears that respondents have reservations about the **idea of a data ownership right in general** — irrespective of the party/parties to whom it would be granted. This is on two grounds of principle and on two grounds related to problems of practical implementation of such a right.

The grounds based on principle are:

(i) Fear of any regulatory intervention in the market. In the view of respondents, the market is better placed to allocate assets than the regulator.

(ii) The belief that introducing a type of intellectual property right would make data sharing more complicated as it increases legal costs of implementation, ultimately leading to less data being shared (risk of greater data scarcity). In this respect, some respondents argued that any system of 'data ownership rights' would need to be accompanied by an obligation to license under 'open' terms.

In terms of problems of implementation of any 'data ownership right', stakeholders cited the difficulty of delineating between personal and non-personal data — personal data not being able to be captured by any 'data ownership right' under the terms of the General Data Protection Regulation — and between 'raw' data and data resulting from an analytics operation.

In addition to the reservations on general grounds, there were specific comments made with respect to all three alternative ideas:

The specific idea of **granting a 'data ownership right' to the manufacturer** (companies active in the production and market commercialisation) was rejected by a number of stakeholders on the grounds that it would only reinforce the current *de facto* control of manufacturers and ensuing lock-in effects going as far as creating new data monopolies. Furthermore, some respondents felt that it may not be compatible with trade secrets protection legislation as the sensor-equipped machine, tool or device may feed back data revealing trade secrets from the company operating it.

Very few proponents of introducing such a right expressed their support in more detail. In general, even those who appeared to support a right being granted to producers of sensor-equipped machines cautioned

that such a solution would only be appropriate in some cases, and even then some sort of shared ownership might be preferable.

The specific idea of **granting a 'data ownership right' to the data producer** (entities that operate sensor-equipped machines, tools or devices at their own economic risk) was conversely seen in a critical light by manufacturers who fear a negative impact on their competitiveness, also in comparison with manufacturers from other parts of the world. This would lead to less investment in data collection capabilities (sensor-equipped, connected objects) and thus be counter to the overall ambition of the initiative. Also it was yet to be proven that 'data producers' would be more likely than the manufacturer to share data collected. Some respondents fear that granting such a right would be made ineffective as the manufacturer is likely to buy back the exclusive right to license the use of the data at the point of sale of the object. Some respondents note that from a 'Big Data' perspective this may actually be desirable as the manufacturer appears to be the most appropriate party to aggregate data on the performance of sensor-equipped, connected objects so that a critical mass for extracting insights can be gathered.

Very few respondents argued in favour of the solution proposed. In sectors in which data-driven innovation is resulting from data collection by a multitude of small economic players (e.g. farmers, motor vehicles), there may be a case for granting an exclusive right to license to the 'data producer'. Respondents see such a solution as empowering data users, in the sense that introducing such a right would help weaken the market power of the manufacturers and allow users to share data with the manufacturers' direct market competitors. According to this view, data producers would gain a strong incentive to share data with third parties, as this option would improve their individual negotiation position.

Some stakeholders noted that beneficial effects would be conditional on agreements between manufacturers and their equipment suppliers.

Individual stakeholders argued that with respect to consumer-generated data, making the consumer the party that has a right to allow access and re-use of their data is possibly the most appropriate way of incentivising consumers to participate in the data economy.

The idea of vesting **joint 'data ownership' rights both with the manufacturer and with the 'data producer'** has also been criticised for possibly unnecessarily restricting contractual freedom, negatively impacting on investment incentives on the side of manufacturers of sensor-equipped objects and potentially leading to greater data scarcity as both the manufacturer and the 'data producer' may not agree to license the use of the data. Despite these concerns, overall respondents could see a number of advantages:

Many respondents took the view that introducing such a right would clarify the legal situation with respect to such data and the mutual rights and obligations of manufacturers and users. This could already support greater data sharing. As with the idea of vesting only the user of the machine, tool or device with a 'data producer' right, respondents see the joint ownership ideas likewise as an solution as empowering data users, helping to address the current imbalance in the data economy.

(g) Creation of an obligation to licence under FRAND terms

Under the **seventh** proposed idea, an **obligation to license the re-use of data under fair, reasonable and non-discriminatory (FRAND) terms** would be created. We asked stakeholders to what extent they could agree to the possible creation of such an obligation for two contexts: data generated by sensor-equipped, connected machines, tools or devices, and data generated in the context of an online platform.

As regards data generated by sensor-equipped, connected machines, tools or devices, 23.9 % of the 251 respondents to this question said that they could agree to such an obligation 'to a large extent', another 25.9 % said they could agree to it to 'some extent' and 15.5 % say that they could agree to it 'to a minor extent'. On the other hand, 34.7 % declared themselves to be entirely opposed to the idea. Figures for the overall number of respondents and for respondents from businesses and on behalf of organisations were largely identical.

As concerns data generated in the context of an online platform, 20.9 % of the 249 respondents declared themselves to agree 'to a large extent' to such an obligation, 29.3 % could agree 'to some extent' and 16.9 % 'to a minor extent'. 32.9 % oppose the idea entirely. Figures for the overall number of respondents and for respondents from businesses and on behalf of organisations were largely identical.

(h) Comparing options

Put in a **comparative perspective**, the **most popular measure** proposed in the Communication is fostering the use of Application Programming Interfaces, with 68 % support, 15.8 % of respondents seeing it beneficial under certain circumstances and only 5.3 % entirely opposed.

The **least popular** possible way forward is the granting of exclusive rights to license the usage of data to one single party, either to the manufacturer or to the 'data producer', i.e. the user of the sensor-equipped, connected machine, tool or device. Both options saw negative reactions of 51.8 % ('data producer right') and 65.8 % ('data ownership right' with the manufacturer') and positive responses of only 30.8 % and 18.3 % respectively.

The remaining possible ways forward fall into two groups. Possible ways forward in the first group gathered a bit more than 50 % in positive reactions ('strongly positive' and 'somewhat positive' reactions), but also a significant share of negative reactions (roughly 30 % in the instant case). These ways forward are:

- leaving it to contractual practice (status quo);
- guidance issued by the Commission;
- recommended contract terms;
- granting a right to license to both the manufacturer and the user of a sensor-equipped, connected object.

When looking also at the detailed comments in the free text fields it is important, however, to understand that some of the possible ways forward (in particular 'guidance' and 'recommended contract terms') received negative reactions also because the measure would not go far enough in the view of some stakeholders. It is not possible to deduce solid numerical information on the proportion of respondents that reacted negatively for this reason.

The second group brings together measures for which positive responses are significant, but never account for more than 50 % of the responses: The ideas to lay down in legislation a set of (cross-sector or sector-specific) non-mandatory contract rules for B2B contracts, to create additional civil law remedies against illicit misappropriation of data, or to create FRAND obligations to license data have seen **some support**, with full support ranging from 23.9 % to 33.6 % and support under certain circumstances between 15.5 and 25.9 % (combined positive replies between 42.2 % — B2B contract rules — and 49.8 % — FRAND). However, both positive response options combined never totalling more than half of the responses, while negative

reactions ranged between 27.6 % — 41.1 % (NB: for the FRAND obligation the answer options differed. The answers for 'to a minor extent' were neither counted as positive nor as a negative reply in this schema).

(iii) Assessing the idea of giving access to privately-held data for public-interest and scientific purposes

The Communication COM(2017)9 also presented the idea that public authorities could be granted access to data where this would be in the 'general interest' and would considerably improve the functioning of the public sector, or to scientists for their use in their research.

With its questions in this section of the public online consultation, the Commission sought to understand to what extent companies could agree to allowing the public sector to draw on data they hold, under what conditions such data could be made available to public authorities, whether this area should become a subject of regulation and if so, at which level.

Among 225 businesses/organisations responding to the section on 'Access for public-sector bodies and scientific research', more than half **could agree to allowing public authorities to access their data** for specific purposes: to prevent public health risks (44.0 %), for access by statistical offices (41.8 %), or for scientific research that is funded from public resources (39.6 %). On the other hand, 34.7 % of respondents said that they could not agree to data sharing for any of the public-interest purposes mentioned.

From responses to the free text field it emerged that respondents overall support the idea of sharing specific data sets with public-sector bodies for the common good under certain conditions. However, some stakeholders identified barriers when sharing their data with the public-sector bodies such as: maintaining security of the IT systems, preserving data privacy, in particular avoiding the tracking of individuals by government authorities, preserving commercial confidentiality and trade secrets; it should be clear that any such data shared would not be transmitted to third countries with additional risks of misuse of the data.

Some respondents were concerned that granting such access may distort the market and have harmful impacts on innovation. Individual respondents pointed to the fact that the data is processed and stored in a way that serves a concrete business need and that may make the data not readily useable for other purposes.

Through additional information put in the free text field, respondents also suggested **concrete solutions that would encourage them to share the data** with public-sector bodies, such as: Creating a reciprocity obligation (similar to licences for free and open source software); establishing clear limitations on the purpose of the use of the requested data; compensating the business/organisation in some way; under the condition that the insights resulting from the processing of their data become publicly available.

Asked about whether companies could agree to **make the data available for free or at the mere cost of dissemination**, only 63.4 % of companies responded. 68.5 % of companies that responded said that they could agree to this, whereas 31.5 % said that they could not agree to sharing data for free or at the mere cost of dissemination.

Some 253 respondents (business as well as self-employed persons and individuals) replied to the question **whether there should be action at EU level** to address access to such data for the entities mentioned in the previous question: 35.0 % replied that the EU should address this issue through legislative measures (for a scope to be defined); 31.5.% replied that the EU should address this issue but only with voluntary measures

(e.g. industry self-regulation); 20.1 % replied that the EU should not address this issue and 13.4 % of the respondents said that they did not know.

Conclusion

In terms of better understanding the level of data sharing in B2B constellations, the results of the public online consultation portray a situation where more data is shared compared to previously available evidence (cf. Staff Working Document SWD(2017)2 accompanying the Communication 'Building a European Data Economy', COM(2017)9, p. 14), both from the demand and supply perspective: 56.9 % of respondents indicate some type of dependency on data produced by others. Three quarters of the 272 respondents to this section share their data to some extent. The majority of these respondents pass on data only inside the same economic group or to a subcontractor. Roughly a third share data more widely, either on the basis of relatively open re-use conditions or against payment of a licence fee.

When asked about obstacles in data sharing experienced, just over half experienced no problems, while 47 % had experienced difficulties. Around a third of respondents feel that neither competition law nor legislation on unfair contract terms or unfair commercial practices fully address such problems. Concerns on fairness of access to data resources appear to be particularly strong in the after-sales market of vehicles. Among concrete suggestions, individual respondents point to recent German draft legislation that would make control over data and the capacity to dominate a market through network effects created (notably by online platforms) part of the assessment of what constitutes a dominant position. Large businesses and organisations representing businesses take the opposite view, namely that competition law is well-equipped to handle the — in their view — few cases of abuse of dominant position and also that limited rules on B2B contracts are necessary in order to provide the flexibility necessary to ensure a return on the investment in data collection (capabilities).

Data holders feel that their investments into data collection (capabilities) are otherwise well protected, notably through the Database and Trade Secrets Protection Directives, and require no additional protection.

When asked about their position on the future evolution of the data economy, virtually all stakeholders agree with the Commission's objective to make more data available for the data economy.

However, when it comes to potential actions to be undertaken by the Commission to make more data available for re-use, most stakeholders call for prudence. They argue that data value chains and business models building on data are very diverse, making it difficult to conceive one-size-fits-all solutions. Virtually no stakeholder believes that there is a need for additional legal protection of data collection (capabilities). Almost all companies or business organisations believe that freedom of contract should prevail so that individual solutions adapt to the concrete needs of a business case. Consequently, these respondents consider that no regulation is necessary.

The idea of an exclusive right to license data from sensor-equipped machines, tools or devices is seen with particular scepticism, mainly on the premise that this would lead to greater scarcity in data supply as a result of increasing legal uncertainty in the practical application and resulting legal transaction costs.

Respondents are, however, favourable if such a right were to be shared among the Original Equipment Manufacturer (OEM) and the user of a sensor-equipped machine, tool or device. In particular representatives of SMEs support such a solution.

As concerns the possible way forward at the opposite end of the spectrum, i.e. creating an obligation to license the re-use of data under fair, reasonable and non-discriminatory (FRAND) terms, this option was overall seen relatively favourably by respondents. 49.8 % agreed either 'to a large extent' or 'to some extent' that this could lead to more data sharing. On the other hand, 34.7 % of respondents, and in particular data-holding companies and their business associations, voiced strong concerns about this solution.

The 'technical' way forward, i.e. fostering the use of application programming interfaces (APIs) received the biggest support. As a number of respondents remarked, APIs are only a vehicle for data sharing and are used when the data-holding company has already made a choice to share data. Representatives of SMEs therefore consider that data holders should be legally obliged to openly document APIs and that legislation could also impose open APIs (i.e. open to a wider number of stakeholders under non-discriminatory terms).

The remainder of the proposed ways forward, the middle-ground solutions, command support by either just over or just under half of the respondents in the online questionnaire. This includes two other soft options, notably Commission guidance on how existing legislation is to apply to new business situations of the data economy, and recommended contract terms. The fact that both solutions are seen sceptically by a not insignificant number of respondents can be explained by the fact that for some sceptical respondents, the solutions are not effective enough whereas for others they may already go too far. In particular 'one-size-fits-all' recommended contract terms are seen with some scepticism by certain stakeholders, but sector-specific contract terms are seen less sceptically. Proposing regulation on default but non-mandatory contract rules for B2B situations, paired with a fairness control, saw a divided response, with 42.2 % agreeing that this solution would make more data available, but a similar number (41.1 %) of respondents disagreed with this solution.

In terms of sector-specific situations, discussions often revolved around access to in-vehicle data in order to enable an after-sales market for products and services and in the field of agriculture. With respect to access to in-vehicle data, the positions of stakeholders are quite pronounced. Original equipment manufacturers cite a number of reasons why access to data to third parties should only be given under certain conditions, e.g. in order to ensure the safety and security of the car. Stakeholders from the after-sales market are deeply concerned about the continued viability of current business models and about the opportunities to develop entirely new business models. For smart agriculture, most stakeholders recognised the importance of clearly respecting the position of the farmer when it comes to exploiting the data generated by him or her.

Although not at the same level of deployment, representatives from the sector of service and repair of other connected (IoT) objects voiced concerns that OEMs may be tempted to readjust service agreements as a result of superior knowledge of clients' needs resulting from data feedbacks.

The idea of allowing access to data held by companies for public authorities for public policy purposes was also seen relatively favourably, in particular with respect to the clearly circumscribed re-use purposes (to prevent public health risks, for access by statistical offices or for scientific research that is funded from public resources). 32.7 % of respondents, however, disagreed entirely. Many company respondents argued that such data access should be fairly compensated, taking into account the investments made in the data collection or adaptation that would be necessary before the data could be used by public authorities (in terms of conversion of data into relevant formats, anonymisation of personal data or of confidential business information).

Liability

This section presents information on current extra-contractual and contractual liability challenges in the context of defective Internet of Things (IoT)/robotics products and services. More precisely, the Commission is trying to investigate primarily the following aspects:

- problems encountered when producers were held liable for damages, and the difficulties in claiming damages from consumers' side;
- the types of damage encountered;
- issues that cause reluctance when buying IoT/robotics devices;
- feedback on the type of liability regime that is best suited to addressing current liability challenges in the context mentioned.

Examining extra-contractual and contractual liability issues for IoT and robotics products and services

Generic considerations on producers' extra-contractual liability challenges

The first set of questions addresses producers of IoT/robotics applications. It tries to gather information on the type of the technological development they encompass in their businesses and, in general, to clarify if these respondents have experienced problems with classifying IoT/robotics as either products or services in order to comply with a specific liability regime.

Out of 138 respondents who answered the question as to which new IoT and/or robotics technological developments they deal with, one quarter mentioned non-embedded software or mobile apps, almost 10 % mentioned smart objects such as thermostats, watches or cars, and 7 % mentioned advanced sensor equipment. 4 % of these respondents mentioned automated cars, while an even smaller proportion of respondents deal with smart medical devices, robots or drones. Finally, almost half (67) of the respondents stated that they deal with technology other than those proposed among the possibilities. This figure, however, includes about 20 larger technology companies and associations that noted they use more than one or all of the proposed technologies in their business activities. Among the technologies mentioned in addition were connected vehicles, chatbots, location, navigation and tracking devices, smart tyres, smart mobility and transport solutions, lighting technologies, smart homes, bookkeeping and tax reporting or middleware for intelligent communication between devices.

Out of the 113 responses, 48 replied that they do not know if they have encountered problems in not knowing in which category (product/service) to classify the device in order to comply with a specific liability regime and 43 answered that they have not encountered any problem. 16 indicated that they have experienced moderate problems with classifying IoT/robotics devices and 6 had experienced significant problems. None of the position papers expressly addressed this question, although the vast majority (42 out of 50) of those that covered liability expressed satisfaction with the current liability framework, believing it adequate to cover new technological developments such as the Internet of Things.

A few position papers (8 in total) did express concerns about the current liability regime. Two industry associations stated in their position paper that products or services are increasingly dependent on other products, services or sensors (not part of the original product) and that when combined with the increasing scale of artificial intelligence and self-learning systems, this will make it increasingly difficult to pinpoint the

responsible party. This point was echoed in the two position papers received from consumer organisations. However, the industry associations argued that at the moment there is not sufficient evidence to make changes to the current liability regime and the Commission should continue to monitor the situation.

The two law firms which responded to the consultation also criticised the current legal framework. One argued that the definition of a product needs to be amended as companies exempt themselves from liability by classifying software products as providing a service.

The four trade associations provided information about how their members solved the issue of classifying something as a product or a service, alongside 5 businesses. Two associations stated that this issue had not been solved: one association highlighted the difficulties encountered with self-certification, while the other stated that work was under way to address this through the review of the Machinery Directive. The other respondents stated that they solved this issue through legal analysis, contractual negotiation and by looking at the problem on a case-by-case basis.

From the respondents to the online questionnaire, 67 from 99 said that they did take into account the possibility of being held liable for potential damages when pricing IoT/robotics devices.

Specific considerations on producers' extra-contractual liability challenges

A second set of questions were also targeted at producers. These tried to investigate in more detail any problems encountered when dealing with liability for damages per type of product, type of damage, and type of liability framework used. One question also investigates the issue of specific insurance to cover producers' liability in case someone makes a claim against them.

Only one business provided details on the issue of damage. The business in question was held liable for damage its smart meter caused to a boiler and this was covered by the business's insurance.

Some 47 respondents out of 60 indicated they did not have specific insurance for IoT/robotic products while 13 stated they did. While none of the position papers directly addressed this question, 6 expressly stated that they were not in favour of introducing compulsory insurance and none of the position papers called for compulsory insurance to be introduced. Two insurance associations warned about the dangers of introducing compulsory insurance.

Consumers' extra-contractual liability challenges

A third set of questions tried to collect information in relation to difficulties encountered by consumers when claiming damages in the context of defective IoT/robotics devices (type of damage suffered; the amount of loss; issues encountered when initiating the procedure for claims).

Some 96 consumers out of 114 said they had not suffered any damage while 18 said they had. Among the latter, 11 stated they suffered a missed opportunity loss, 5 a pure economic loss, 3 had suffered damage to property and 3 listed their loss as 'other'. Position papers submitted by consumer organisations mentioned other types of losses (the destruction of digital content and companies losing consumers' personal data or unauthorised third parties gaining access to consumers' personal data).

Only two companies answered the question related to other types of damage suffered not listed by the questionnaire — one company mentioned that their data was hacked and the other stated that "The unavailability / defects of the IoT-based devices, which participate in the performance indicators of our own services rendered to customers, have resulted in our own commitments to our customers".

Only one company and two individuals provided answers to the question referring to the amount of losses suffered. The company said their losses were significant and the individuals suffered a loss of less than 100 euros.

Only 2 respondents stated they had made a claim, 14 said they didn't.

The question relating to the decision on whether a claim was actually made gathered 15 replies in total. 12 stated they did not make a claim because the procedural costs were too high, 2 mentioned they had no right to claim damages despite the losses suffered and 1 did not know that a claim could be made.

Only one respondent from the online consultation answered the question in relation to the reasons why it was difficult to make a claim. It was specified that the most difficult aspects of the process were the time involved and the costs of the ordinary court.

However, the position papers submitted by law firms and consumer organisations indicated that the main difficulties consumer face when bringing a claim are in establishing that the product was defective, establishing the causal link between the defect and the damage, and the fact that the definition of damage is too narrow. In particular they highlight the problem that consumers face in proving that software does not provide the safety that they are entitled to expect.

Software security issues and reluctance to buy IoT/robotics devices

A fourth set of questions tried to gather information on issues that make consumers reluctant to buy IoT/robotics devices or on digital issues relating to the functioning of such devices, such as software security problems (e.g. failure of the software, cyber-attack). This set of questions also collected information on more general liability issues, like the necessity for installation of event data recorders; identification of specific national rules on liability for damage caused by the new technological developments or on who should bear the liability in the case of damage caused by defects or by a smart device, which combines tangible goods (a car), digital goods (an app) and services, malfunctioning.

A large majority of the respondents (76) had not experienced a software security problem. Approximatively a third (41) did face such security problems. Nevertheless, a few of them (17) admitted not knowing the exact cause of such problems. According to the few respondents that answered the question on the main causes of security failure (10), the following problems were listed:

- inability to install/use a purchased device after hacking of a digital media entertainment service, which lasted 4 weeks;
- security vulnerability and no responsibility from manufacturer, seller or importer;
- extraterritorial nature of software/hardware products, which makes it difficult for the buyer to get in touch/control the manufacturer;
- data hacked, caused by software vulnerability;
- cyber-attack through insufficient security features of the device;
- improper use of encryption.

Among all the respondents, the majority (69) did not really have any significant difficulty with updating their devices' software, either because the updating process was quite easy or at least manageable for almost half of them (46), or because they do not even need to update those devices by themselves (23). However, 24 respondents admitted having faced difficulties in updating their devices.

One manufacturer from the aviation sector highlighted the fact that in their sector the purchase of software is usually bundled with support and maintenance service. In addition, if the software is developed internally or is specially designed for them (implying that they require full access to its source code), they can update the software internally provided that they have full access to its source code.

On the question related to reasons for a potential reluctance to buy IoT products, 247 replies were received, among which most were from businesses or organisations (179), with a substantial proportion also from individuals (60). For the majority, the two main concerns regarding IoT products or services are the risks in terms of security/cybersecurity (63) and the risks in terms of privacy (59). The number of answers is quite similar when it comes to the other following reasons justifying a possible reluctance to buy IoT products or services: 26 considered such hesitation is due to the price of these products or services, 25 to the uncertainty about the cause of potential damage and 23 to the uncertainty on whether they would receive compensation in the event of such damage. Several position papers pointed out as well the legal uncertainty that IoT entails, but the majority argue that these issues could be solved through contractual arrangements. For most of them, a potential Commission intervention should be limited to developing non-binding guidance or best practices. However, a few position papers advocate a real clarification and/or adjustment in this area (e.g. Arthur's Legal, BEUC-Bureau Européen des Unions des Consommateurs).

It also has to be noted that a few of the respondents (24) also replied that they are not reluctant to buy IoT products and services. Among the reasons for reluctance, 3 out of 9 respondents to this question highlighted the lack of interoperability/compatibility as a barrier for IoT acceptance. The Austrian Chamber of Labour (Bundesarbeitskammer Österreich) pointed to the lack of transparency regarding the way these devices actually operate: legislative action may therefore be needed to regulate this aspect. Another argument, cited this time by the French Electricity Transmission Network (Réseau de Transport d'Electricité), is the difficulty to adapt IoT technologies designed for the tertiary sector (smart grids/meters, smart home solutions, etc.) to the public transport network.

The vast majority of respondents reported that there are no specific liability rules for damage caused by new technological developments, with the exception of the recently revised German Road Traffic Act (which includes specific provisions for automated driving). BEUC is of the opinion that it is high time to update the current Product Liability Directive in light of these new technological developments. An association of automated suppliers argues in favour of event data recorders and against being held responsible for failures of the overall system.

In relation to the question on who should bear the liability in the case of damage caused by smart devices combining tangible goods, digital goods (app) and services (e.g. data services), no clear picture emerges. A substantial but equal number of respondents support joint liability of all parties involved in the production of a product, individual liability of each component producer or liability of the end producer/system integrator. BEUC, the German and the Portuguese Associations of Consumer Protection and the ADAC argue that since it could be extremely difficult for the end customer to identify what part of a smart device malfunctioned, he/she should be able to address compensation claims to the end producers. A significant number of

respondents believe a uniform solution will not be possible and call instead for case-by-case analysis. A few respondents call for new risk management schemes that would maximise overall societal benefit.

Some 60 % of the 138 respondents to the question (consumers/users) believe that IoT/robotics devices should be equipped with an event data recorder to track what the device was doing when the damage occurred.

Examining possible options and ways forward

Considerations on tools and regimes to deal with IoT/robotics liability challenges

A first set of questions gathered information on generic questions related to: 1) the type of liability regime to be used to minimise or avoid the realisation of the risk; 2) who should bear the liability in the case of damage caused by defects or malfunctioning of a smart device which combines tangible products, digital products and services; 3) the type of liability regime (contractual or extra-contractual) seen as the most consumer-friendly way to deal with damage caused by defects or malfunctioning in smart devices, which combine tangible products, digital products and services; 4) assessing whether IoT/robotics challenges require an ad hoc approach at EU level.

As to who should bear the liability for defects of a smart device, there were 134 replies from organisations, businesses and individuals, mostly from Belgium (27) and Austria (27), followed by Germany (18) and France (14).

Most of the replies (29) argued that the manufacturer or producer should bear liability, whereas some of the replies limited that statement to the producer of the defective device. 26 replies stated that no change to the current legal situation was needed and 23 replies advocated the allocation of liability on a case-by-case basis. 14 respondents provided an identical response, stating that established standards should not be changed and that due to the documentation ensured by log files, detailed proof would be available indicating which component caused a certain reaction.

In response to the question whether attribution of liability in the context of IoT/autonomous systems products and services can adequately be dealt with through contracts, 47 answered yes, 69 answered partially and 45 said that attribution of liability cannot be dealt with through contracts.

From the 50 position papers that addressed the question of liability, 32 said that the liability frameworks as a whole (contractual and extra-contractual liability) are adequate to deal with the challenges resulting from new technologies such as IoT and autonomous systems.

Some 133 businesses, organisations and individuals replied to the question assessing whether an ad hoc EU level approach is needed. The majority of the respondents were from Austria (27), Belgium (25), France (17) and Germany (17). The vast majority of the respondents (78) do not see a need for an ad hoc approach at EU level. 28 respondents advocated such an approach, whereas the remaining respondents did not express a clear position or expressed the view that the situation should be assessed further before deciding on further action.

Considerations on other possible ways forward to deal with the liability challenges of emerging technologies like IoT and robotics

A second set of questions tries to identify other possible way forward in relation to IoT/robotics liability questions, like liability caps; safety standards, mandatory cyber insurance, insurance contracts; to assess the current legal framework for algorithms (degree of protection insured; the need for standard certification or test bedding; who should bear liability for defects caused by products embedding open algorithms).

In relation to the question on the need of a liability cap, i.e. an upper limit to the compensation of damage, 37.4 % said no, 21.8 % said yes for all IoT products, 20.4 % did not know, 15.5 % said yes but only for specific products abiding by strict safety standards and 4.9 % said yes but only for specific products in the experimentation/testing phase. In addition, 41.5 % of respondents do not believe that safety standards can replace liability tools, while 23.5 % replied that they did not know. 20 % agreed for all IoT products, 10 % agreed but only for products performing automated actions or taking independent decisions and 5 % agreed but only for specific products in the experimentation/testing phase. In relation to the question on a need for mandatory cyber insurance, 43.1 % responds believe there is no need, 22 % said yes for all IoT products, 21.1 % did not know, 12.4 % said yes but only for products performing automated actions or taking independent decisions, and 1.4 % said yes but only for specific products in the experimentation/testing phase.

Most respondents (6) stated that the producer of the physical device jointly with the provider of the digital content should take out such insurance contracts. Among the respondents who chose 'other' as their response, one respondent stated that the user of the devices should also take out such contracts. Secondly, some respondents (3) pointed out that the complexity of the question requires different approaches, like a risk management approach or a combination of the proposed options. Two respondents also specified that pharmaceutical injuries insurance and vehicle insurance can be used as reference points.

Three strong views have emerged in relation to the assessment of the current legal framework (both business-to-business and business-to-consumer) for algorithms, e.g. when it can be proven that an accident has been caused by a bug in the algorithm. Some respondents stated that the current legal framework provides sufficient protection (13), especially under the Product Liability Directive, national tort law or contractual instruments. One respondent cited the Finnish liability system, which provides efficient remedies. Elsewhere it was stated that there is not enough legal certainty (9). Some respondents pointed out that the aggrieved party may face difficulties in enforcing their rights due to information asymmetry and the burden of proof to the user's disadvantage (10).

A majority of respondents believe that government-led certification of algorithm-based services is not desirable and feasible because of the great diversity of algorithms, the danger of disclosing sensitive company secrets and the negative impact on innovation. If certification and standardisation is to be done, it should be industry-led.

As to who should bear the responsibility in the case of a defect in open algorithms, a significant number of respondents want to allocate responsibility either to the producer of the algorithm or the user (who decides to incorporate the algorithm in a final product); a clear preference between these two options cannot be observed. A substantial number of respondents claim that the allocation of responsibility should be handled on a case-by-case basis.

Conclusion

Overall, this section sought to collect information on extra-contractual and contractual liability challenges in the context of IoT products and services and autonomous systems and advanced robotics. It has to be taken into account that the results of the consultation do not represent the entire ecosystem[1], so further assessment is needed, taking into account the findings gathered so far.

In terms of the technological development provided by the respondents (138), one quarter mentioned they provide non-embedded software or mobile apps, almost 10 % mentioned smart objects such as thermostats, watches or cars and 7 % advanced sensor equipment. 4 % of these respondents mentioned automated cars, while an even smaller proportion of respondents deal with smart medical devices, robots or drones. Finally, almost half (67) of the respondents state that they deal with technology other than those proposed among the possibilities. This figure, however, also includes about 20 larger technology companies and associations that use more than one or all of the proposed technologies in their business activities. Other technologies mentioned were connected vehicles, chatbots, location, navigation and tracking devices, smart tyres, smart mobility and transport solutions, lighting technologies, smart homes, bookkeeping and tax reporting or middleware for intelligent communication between devices.

In relation to the liability challenges pointed out by producers in the context of IoT and robotics, the picture that emerges is that businesses have not encountered difficulties, or that they do not know if they have encountered problems. Only 16 producers have experienced moderate problems with classifying IoT/robotics devices as products or services and 6 had experienced significant problems in this respect. Two associations stated that this issue had not been solved: one highlighted the difficulties with self-certification and the other stated that work was under way to address the problem through the review of the Machinery Directive. The other respondents stated that they solved the classification issue through legal analysis, contractual negotiation and looking at the problem on a case-by-case basis. Only one producer gave an account of having been held liable for damage their smart meter caused to a boiler: this was covered by their insurance.

For liability challenges pointed out by consumers, the emerging trend is that most of the consumers have not suffered damage from defective IoT/robotics products and services, with only 18 out of 114 respondents acknowledging having suffered damage. Among the latter, some trends emerge:

- Of the types of damage suffered that are not covered by the current Product Liability Directive, the respondents listed missed opportunity losses (11) and pure economic losses (5). As for the remaining types of damage, only 3 stakeholders listed damage covered by the Product Liability Directive, such as damage to property and other types[2].

- In relation to the amount of losses suffered, there is a mix between low and high losses[3] .

[1] For example: the total number of contributions in general is limited and for certain questions only 3 contributions were provided. In addition, different stakeholders provided identical responses to certain open questions.

[2] One company mentioned that their data was hacked and the other stated that 'defects of the IoT-based devices'. In the position papers from consumer organisations, other types of loss mentioned were the destruction of digital content and companies losing consumers' personal data, or unauthorised third parties gaining access to consumer's personal data.

[3] One company mentioned that their losses were significant, while 2 individuals suffered a loss less than 100 euros.

- In relation to the causes behind whether a claim for compensation was actually made, 12 out of 15 respondents stated the reason was the high costs of the procedures, 2 respondents stated they had no right to claim damages and 1 said they did not know a claim could be made.

The position papers from law firms and consumer organisations indicate that the main difficulties consumers face when bringing a claim are in establishing that the product was defective, establishing the causal link between the defect and the damage, and the fact that the definition of damage is too narrow. In particular they highlight the problem that consumers face in proving that software does not provide the safety that they are entitled to expect.

In relation to the investigation on the causes that make consumers reluctant to buy IoT/robotics devices, the following trends emerge:

- a large majority of the respondents (76 out of 117) did not experience software security problems;
- the majority (69 out 112) did not really have any difficulties updating their software devices;
- among those respondents (10) who answered the open question on the main causes of security failure, the following problems were listed: inability to install/use a purchased device after the hacking of a digital media entertainment service, which lasted 4 weeks; security vulnerability and no responsibility assumed from manufacturer, seller or importer; extraterritorial nature of software/hardware products, which makes them difficult to control the buyer; data hacked, caused by software vulnerability; cyber-attack through insufficient security features of the device; improper use of encryption;
- the two main concerns regarding IoT products or services are the risks in terms of security/cybersecurity and the risks in terms of privacy.

As for the type of liability regime that could best respond to the legal challenges posed by IoT and robotics, the following trends emerge:

- A majority of respondents, in particular trade associations and consumer protection organisations, believe that contractual liability alone is insufficient in addressing liability questions arising from smart devices.
- A significant number of respondents, mainly individual companies, believe that contractual liability is sufficient and offers flexibility which an extra-contractual solution to liability questions could not offer. In particular, they fear that new extra-contractual liability rules may harm innovation.
- The vast majority of position papers which expressed a view on liability believe that the current framework is adequate to deal with issues arising as a result of emerging technologies.
- A vast majority of the respondents do not see a need for an ad hoc approach at EU level.

As to who should bear the responsibility in the case of defects of smart objects/IoT/robotics devices, following picture emerges:

- A substantial but equal number of respondents support joint liability of all parties involved in the production of a product, individual liability of each component producer or liability of the end producer/system integrator.
- Consumer associations such as BEUC, the German and the Portuguese Associations of Consumer Protection and the ADAC argued that since it could be extremely difficult for the end customer to identify what part of a smart device malfunctioned, he/she should be able to address compensation claims to the end producers, as is currently the case under the Product Liability Directive.

- A significant number of respondents believe a uniform solution will not be possible and call instead for case-by-case analysis.
- Some respondents (albeit few) call for new risk management schemes that would maximise overall societal benefit.

While the appetite for changing the current liability regime is limited in general among stakeholders, a few stakeholders, mainly from the consumer side such as the BEUC, believe an overhaul would be beneficial and necessary.

Portability of non-personal data, interoperability and standards

The main objective of this section was to gain insight into the current possibilities for businesses to port the data they have provided to their service providers, as well as the opportunities and potential adverse effects of portability of non-personal data.

The Commission also wanted to learn more about existing practices and preferences regarding standards to support interoperability (especially in the cloud computing context), and to gain insight into the respondents' standardisation priorities, as well as their preferred options for implementing such priorities.

Four main policy options were tested on the respondents in this section:

- the introduction of a portability right for non-personal data regarding cloud services;
- the introduction of a portability right regarding non-personal data generated by sensor-equipped machines, tools and/or devices;
- the introduction of a portability right for non-personal data regarding online platforms;
- the definition of a reference architecture recommending a standardised high-level framework identifying interoperability interfaces and specific technical standards for facilitating seamless exchanges across data platforms.

Although the consultation questions focus on aspects related to non-personal data and/or B2B contexts, this section was open to any type of respondent.

Portability of non-personal data

The section on portability of non-personal data was responded to by a total of 296 respondents, of which 261 represented businesses (including self-employed individuals) and 35 were individuals responding in their personal capacity.

Data portability practices

Out of the respondents to the portability section of the consultation, 54.3 % said they are using or had used services allowing the portability of non-personal data that they had previously provided to the service. Different types of cloud services were most frequently mentioned as the context for porting data, along with different kinds of online platforms. The majority of respondents (73.1 %) were either neutral (43.1 %) or satisfied (30 %) with the current conditions. Among those less satisfied (26.9 %), the lack of, or insufficiency of, standards on how to port data, as well as the lack of interoperability of formats and semantics, seem to be the two main reasons for dissatisfaction with the conditions for data portability. Other reasons mentioned were also technical in nature, such as the lack of possibilities to upload the data to another

service once extracted and difficult demand for anonymisation or pseudonymisation of data. Contractual issues such as unclear or changing contractual conditions were also mentioned by some respondents.

When asked about their experiences with switching cloud services or online platform providers, 29.6 % of business respondents said they have experienced difficulties, while 70.4 % reported either not having experienced such difficulties or not having been interested in switching. Of the respondents who expressed the intention to switch, roughly 45 % encountered difficulties. It should be mentioned in this regard that both providers and users of cloud services answered the question, making it impossible to discern clear issues that could exist between the groups of providers and their users.

The image changes when only answers by SMEs are taken into account. 40.3 % of all SME users have experienced difficulties in switching providers. In line with the figures above, this percentage does not take into account whether SME users were interested in switching providers or not. Bringing this element into the analysis, it emerges that 71 % of SME users have had the intention to switch providers. Limiting the calculation to this latter group, it emerges that 56.8 % of them experienced difficulties with switching providers. This shows that more than half of the SME respondents who had the intention to switch providers experienced difficulties with this.

When looking at the issues that could be behind the problem, as many as 85.1 % of all business respondents and 91.6 % of SME respondents said the possibility to port non-personal data was an important factor. Other issues reported were lack of interoperability/compatibility (11 respondents), lack of consistently applied standards (7 respondents), lack of APIs or tools to import and export data (5 respondents) and high exit/migration costs (10 respondents).

In general, both businesses and individuals perceive the most important advantages of data portability to be the ability to build value deriving from the data (53.2 %), to switch providers (52.86 %), and to give third parties access to the data (42.09 %). There were multiple answers possible, and many respondents opted for several answers. When asked to specify additional advantages of portability of non-personal data, 17 respondents mentioned the ability to introduce new business models, services or products and 17 respondents mentioned the positive effect such portability would have on competition in the market.

Of the respondents representing businesses, 40.9 % said their business offers portability of non-personal data to their clients. However, few respondents gave concrete examples when asked about the conditions under which they grant such portability. Of those who did respond, 6 claimed to offer free portability of either all their data or all non-personal data. These were mostly organisations and research bodies. Another 5 reported offering portability as a paid service. When asked to give good examples of services offering data portability, many respondents gave examples, but few were repeated by several respondents.

The perceived need and possible effects of portability of non-personal data

Some 49.8 % of the 255 participants agreed that there is a need for businesses to receive non-personal data in a machine-readable format and be able to license the use of such data to any third party. However, only 114 respondents have a clear idea which types of data should be covered by an enlarged portability right. 41.8 % believe that such a right should also cover data generated by sensor-equipped machines, tools and devices [*49 respondents out of 117 overall; NB: taking away the 'no answers', 30 % ticked the box for this answer option; however, the answer options were mutually exclusive and an additional 13 signalled in the open response field that they support all three options*], while only 26.5 % take this view for cloud service

providers and 27.4 % for data submitted to online platforms [*same for adding the 13 respondents that signalled support for all three options in the open question field*].

It emerged from the analysis of the written input that most stakeholders are concerned about the introduction of a right to data portability to any kind of data held by a company, whereas the consultation had specified three cases (data generated by sensor-equipped machines, tools or devices; non-personal data submitted to a cloud provider; non-personal data submitted to online platforms).

Stakeholders advise looking on a sector-by-sector basis to determine where there is true demand for a portability right, as introducing such a right may raise prices for products and such a rise in prices would only be justified if there is a benefit on another side. The cloud sector is often mentioned as benefiting from the introduction of a portability right, as mentioned by stakeholders representing industrial sectors such as transport, energy and utilities. Academics and stakeholders from the financial sector were also cautiously positive about the introduction of data portability rights in the cloud context.

On the introduction of general portability rights (i.e. not cloud-specific), many suggest observing first how the right introduced in the GDPR Article 20 will be applied in practice. Soft measures such as guidance instruments or codes of conduct might be more appropriate at this stage, while economic operators could use the contractual freedom to grant such rights or not, depending on the business model. Some stakeholders also consider it hard to separate personal data (subject to a right to data portability) from non-personal data. Stakeholders and telecoms firms in particular have flagged as potential issues considerable adaptation costs with respect to systems which do not distinguish between 'raw' data and data subject to some form of processing. Similarly, commercial interests and trade secrets would need to be adequately protected. Some stakeholders suggest presenting soft measures such as guidance instruments or codes of conduct before adopting fully-fledged legislation on a broader right to data portability.

Possible effects of different options for data portability rights

Although a majority of respondents said yes or were undecided regarding a need to introduce a general data portability right (regarding non-personal data generated by sensor-equipped machines, tools and/or devices), a substantial number of respondents pointing out potential negative effects. Positive effects mentioned are: improved possibilities of accessing and sharing information (12 respondents), reduced vendor lock-in (11 respondents), new business opportunities (10 respondents) and more data-driven innovation and research (7 respondents). Among the negative effects mentioned are: increased financial and technical burdens on operators (17 respondents), reduced incentives to innovate (12 respondents) and the possible disclosure of IPR and trade secrets (5 respondents).

When asked about a possible right to portability of non-personal data on online platforms, the respondents gave similar answers to those above, although with more focus on reduced vendor lock-in (17 respondents) and less so on new business opportunities (1 respondent) as positive effects. Respondents also mentioned convenience for users (7 respondents) as a positive effect. The negative effects mentioned for this option were similar to those cited above for a general data portability right.

The picture looks slightly different when it comes to a possible portability right in the cloud context. Although many of the effects cited were the same as for the above-mentioned options (the general portability right and the portability right for online platforms), more respondents contributed to this question, and more respondents cited reduced vendor lock-in (35 respondents) and increased competition

(29 respondents) as positive effects. The aspect of improved possibilities to access and share information was not mentioned, but respondents also cited convenience for users (10 respondents). For the other positive effects mentioned above the response regarding cloud was similar. Negative effects from a data portability right in the cloud context were similar to those cited for the other two portability right options.

The effect on innovation seems to be a contentious issue for all three options. Respondents seem to disagree on the possible effect on innovation of data portability rights. Another such issue is the possible effect on competition of the different portability rights mentioned: on the one hand, many believe portability rights for non-personal data would increase competition between service providers and level the playing field, especially for new market entrants and SMEs. However, many also flag possible negative effects on EU companies' competitive edge on the global market, where non-EU competitors may not be bound by the same constraints. Both innovation and competition effects are clearly aspects that are difficult to measure. Opinions on what is good and bad for innovation generally vary.

Conclusions

About one quarter of respondents said they were dissatisfied with the conditions under which they can port data. Furthermore, only about one third of respondents claim to have **experienced difficulties with porting data**.

However, looking at the responses received from SMEs, the picture changes. 56.8 % of SME respondents who had expressed their intent to switch cloud services providers reported having experienced difficulties with doing so. When examining the issues that could be behind the problems, as many as 91.6 % of these respondents said the possibility to port non-personal data was an important factor.

Overall, many respondents from every respondent category **agree that there is a need to facilitate portability of non-personal data,** something which may indicate that they see this being an issue in the future.

When it comes to the possibility of the Commission introducing principle-based rights to **cloud-specific data portability**, many respondents are positive, including from industrial sectors such as transport, energy and utilities. The financial sector and academics were cautiously positive.

When it comes to the **overall attitudes towards the possible introduction of general portability rights** to non-personal data, most respondents urge the Commission to **tread carefully** when promoting general portability rights to non-personal data, suggesting it might be wise to wait for the implementation of the GDPR in order to see how the right introduced in Article 20 of that Regulation will be applied in practice. Reference to the GDPR, and the difficulty in separating non-personal data from personal data, is often made by respondents.

Many respondents, including most of the large industrial companies and industry organisations, believe the implementation of general data portability is best left to the industry itself to solve, either by **contractual or technical solutions and industry-led work on standards**. One industry organisation also suggested that a more effective action for the Commission to take in this area is to work on **skills development**, especially for start-ups and SMEs.

It is important to note that many respondents concentrated on the business-to-consumer (B2C) or business-to-data subject aspects of data portability, even though the **Communication on Building a European Data**

Economy clearly focuses on B2B aspects. This could possibly be because the public debate around portability issues has revolved mainly around the portability rights of consumers and data subjects rather than the possibilities for business users to port data.

Interoperability and standards

The section on portability of non-personal data was responded to by a total of 260 respondents, of which 237 represented businesses (including self-employed individuals) and 23 were individuals responding in their personal capacity.

Issues in the context of cloud computing

When asked **whether they offer standard-compliant solutions,** 61.5 % of the cloud service provider respondents claim to do this. However, they provide very little explanation about this in written answers.

In response to the question **whether they prefer standard-compliant cloud solutions, the user category responded with a convincing majority** — 81.5 % of the user respondents prefer such solutions. In answer to the question **on which specific standards they envisage basing their cloud infrastructure on,** several respondents replied that they preferred open standards in general (in accordance with the definition set in the European Interoperability Framework version 1.0).

There were **several examples of standards mentioned**, among them being PCI DSS, OASIS Tosca standard, Cloud Security Alliance, NIST, COBIT, SSL, SAML, REST, APIs, XML/CSV files, Cloud Control Matrix (CCM), PostgreSQL & Tomcat, CNH Industrial standards; standard formats like XML, GFTS, TXT, JSON, HDFS, Transmodel 5.1, Netex, ISA S88 und ISA S95, Oauth2, OpenID Connect and UMA (Kantara: User Managed Access). Among the ISO standards mentioned were ISO 27018; ISO / IEC 27001, ISO / IEC 27002 and ISO / IEC 27017 on cloud security, together with controls on the protection of personal data of ISO / IEC 27018, as well as UIT-T DMTF, ISO (SC 27 and SC 38) and ITU-T, DMTF, ISO/IEC JTC 1 (SC27 and SC38). One respondent from the automotive industry (HaynesPro) explained that current approaches under ISO are focusing only on the server-side part and miss out the standardisation inside the car for direct access to real-time data as well as direct access to the customer via a standardised API (a standardised but functionally equivalent solution to e.g. Google Android Auto and Apple Car Play). This was a coordinated response left by about 15 respondents.

The **reasons for users to request standard-compliant solutions** are mainly security, data and privacy protection (152 of respondents) and service interoperability (151 respondents). Other reasons pointed out include data portability (115 respondents), SLAs (93 respondents) and cloud management (88 respondents). One respondent explained that the most common considerations both for cloud providers and cloud users when choosing to provide, respectively use, standard compliance services relate to assurances over interoperability, security and privacy.

There were several reasons specified for such a choice, among them privacy security and data protection as key principles of the organisation, lower implementation costs, usage of open technologies (based upon OpenStack or Cloud Foundry), homogeneity of solutions, compliance guarantees and cost reduction.

Priorities

When asked about technical priorities for facilitating data access and discoverability, common metadata schemes were by far the most popular (162 respondents). Of the other options, 106 cited data catalogues, 104 cited common identifiers and 91 cited the use of controlled (multilingual) vocabularies as priorities. The possibility to choose several options for this question led to respondents giving several priorities. In the open response section added to this question, general standards development (8 respondents) and the promotion of APIs (6 respondents) were most often cited as priorities, followed by different kinds of interoperability and security.

When it came to the technical instruments respondents would use to implement their priorities, improvement of existing standards (136 respondents) was by far the most cited, followed by recommendations (102 respondents) and the definition of new standards (95 respondents). Many respondents specified they would prefer non-binding standards to binding ones, and from the position papers addressing issues of standardisation it seems most would prefer industry-led standardisation work to EU-led work. Several respondents have urged the Commission to look to already existing standardisation bodies' work for inspiration or to further build on such work. Existing work in specific sectors such as energy and transport was also mentioned in this regard.

Under the heading of legal instruments, guidelines were the option preferred by most respondents (120 respondents), followed by EU regulation (105 respondents) and support actions (80 respondents). However, many respondents stated in the open response section added to this question that they would generally discourage the introduction of legal actions such as legislation or standard contract terms, or that the Commission should support work on standardisation rather than introducing new legal instruments.

Reactions to the option of a reference architecture

The respondents were asked whether they saw any need to establish a reference architecture recommending a standardised high-level framework identifying interoperability interfaces and specific technical standards for facilitating seamless exchanges across data platforms. To this question 61 % of the respondents said yes and 39 % said no. Several respondents said this kind of reference architecture would improve data sharing processes and ensure a level playing field for market actors. However, many respondents highlighted that this kind of work is already ongoing (among the examples given were ISO/IEC, OASIS, IETF, DMTF, OpenStack) and that there is no need for EU action. Many argued that this kind of work should be left to the industry, or that no reference architecture should be made binding. Some claimed such a solution might limit innovation.

Conclusions

Interoperability is a pressing issue for many of the respondents, and there seems to be consensus around the need for interoperability standards.

Some 81.5 % of the cloud user respondents prefer standard-compliant solutions, and generally also open standards. A plethora of examples were given of standards relevant to cloud computing, including standards on access, data formats, cloud security, data protection and APIs. The reasons for cloud users to request standard-compliant solutions are mainly security, data and privacy protection.

When asked about technical priorities for facilitating data access and discoverability, common metadata schemes were by far the most popular among all the respondents. More respondents would prefer improvement of existing standards over the setting of new standards, but many would also welcome

recommendations as a technical instrument to implement their priorities. Under the heading of legal instruments, guidelines were the option preferred by most respondents, followed by EU regulation and support actions.

Judging from comments given in the open sections in the questionnaire, as well as in the position papers sent in reply to the consultation, a large portion of the respondents believe that the development of standards should be left to industry, or that the Commission should look to already existing work (both horizontal and sectoral efforts were mentioned) on standards before launching new standardisation actions. It is also worth mentioning that many respondents have stated their preference for technical solutions to the data economy issues rather than legal or policy solutions.