SYNOPSIS REPORT CONSULTATION ON THE 'BUILDING A EUROPEAN DATA ECONOMY' INITIATIVE

Introduction

The consultation process on the European data economy, a wide-ranging stakeholder dialogue, was launched with the adoption of the Communication on Building a European Data Economy (COM(2017)9) and accompanying Staff Working Document (SWD(2017)2). The initiative aims to foster the best possible use of digital data to benefit the economy and society. It addresses the barriers that impede the development of a European single market with a free flow of data and legal issues surrounding access to and transfer of data, data portability and liability of primarily non-personal, machine-generated digital data.

The main consultation action was the online public survey which ran from 10 January to 26 April 2017. This covered the different parts of the Communication[1].

The **annex** is a more detailed, qualitative analysis of the results[2] and position papers received. A summary report of this consultation has already been published, providing preliminary trends.

Several horizontal and sector-specific workshops have also been held, either targeting a specific group of stakeholders or addressing a specific issue.

This synopsis report summarises the stakeholder dialogue.

Online public consultation

The stakeholders targeted were businesses of all sizes and from all sectors, including 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 garnered a total of 380 responses, including 332 from businesses / organisations, 6 from self-employed individuals, and 42 from citizens. Most contributions came from private organisations.

In addition, some 18 standalone contributions (i.e. not complemented by replies to the questionnaire) were received (available online). Their authors represent national authorities, companies, national or European business associations, insurance associations, and lawyer representatives in EU and the US. Most of these papers tackle the different sections of the consultation, with a strong focus on access to and transfer of data.

The European Political Strategy Centre (EPSC) also held a public hearing on the European Data Economy.

Workshops

The European Commission (EC) has held a series of workshops addressing specific data economy challenges. Some have been non-sector-specific, while others have targeted a specific category of stakeholders or a specific sector (more information). Their findings are taken into account in this report, set in the context of

[1] A public consultation on the overall evaluation of the application of the Product Liability Directive (85/374/EEC) was held in parallel.

[2] https://ec.europa.eu/eusurvey/publication/European-Data-Economy-Consultation

the online consultation results. The workshops and events relevant to the consultation process are as follows:

Non-sector-specific workshops

- Workshop on Switching Between Cloud Services Providers, 18/5/17, more information
- Workshop with Member States representatives on the emerging issues of the data economy, 31/5/17, more information
- Data access & data sharing: the real impact on SMEs' and start-ups' business models, 29/5/17, more information
- Data access & transfer with a focus on APIs & industrial data platforms, 8/6/17, more information
- Data Economy Workshop, Digital Assembly, 15-16/6/17, more information
- Access to commercially-held data of public interest for public bodies, 26/6/17, more information
- Liability in the area of autonomous systems & advanced robots & Internet of Things systems, 13/7/17, more information

Sector-specific workshops

- EIP-AGRI Workshop on Data Sharing, 4-5/4/17, more information
- Data-related issues in mechanical engineering (6/4/17), medical devices (25/4/17), business services (4/5/17), the automotive sector — Gear2030 (10/5/17), the food & drink supply chain (1/6/17), more information
- Workshop on the transformative effect of access & reuse of data for smart industries, 6/6/17, more information

Next steps

Adopted in May 2017, the Communication on the Mid-Term Review of the Implementation of the Digital Single Market Strategy announced that the Commission would:

- by autumn 2017, subject to Impact Assessment, prepare a legislative proposal on the EU free flow of data cooperation framework which takes into account the principle of free flow of data within the EU, the principle of porting non-personal data, including when switching business services like cloud services as well as the principle of availability of certain data for regulatory control purposes also when that data is stored in another Member State;
- in spring 2018, based on an evaluation of existing legislation and subject to an Impact Assessment, prepare an initiative on accessibility and re-use of public and publicly funded data and further explore the issue of privately held data which are of public interest;
- also further analyse whether to define principles to determine who is liable in cases of damage caused by data-intensive products;
- continue to assess the need for action concerning the emerging data issues as identified in the data Communication from January 2017, such as data access rights.

The consultation process on the Data Economy has confirmed the relevance and importance of all the measures anticipated by the Commission.

Results of the consultation process

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

The consultation process has proven useful for the Commission's work on data localisation and the free flow of data. The outcomes easily meet usability criteria as regards the number and diversity of respondents and the quality of their responses. As 88 % of the 380 respondents are associated with businesses or organisations that have agreed to their identities being made public, it has been possible to conduct economic analyses of specific sectors. In combination with the results of the structured dialogue sessions with the Member States, this allows for a balanced view.

A number of aspects of data localisation measures can be quantified thanks to the consultation results. Most respondents know about the existence of specific data localisation restrictions; most noted that their organisations are obliged to abide by such restrictions.

There is a broad consensus among stakeholders about the impacts of data localisation requirements; very few see no such impact. For all possible categories of impacts tested, most respondents identified high impacts, followed by medium impacts. A few referred to low impacts. As regards the specifics, the main impact of data localisation is found to be on costs, on launching a new product or service and on entering new markets. The types of costs incurred are mostly administrative or arise from duplicated resources in different EU countries. A large majority of respondents point to the recurrent nature of these costs, some mentioning that they have a particularly detrimental effect on start-ups and SMEs. This applies predominantly to resource duplication. Start-ups and SMEs will be unable to compete with incumbents under the increased costs as a result of duplication they have to do.

More than half of respondents think data localisation restrictions should be removed. Most SMEs confirm this, while a very small minority advocate the reverse. Asked to justify localisation restrictions, respondents mention public security, law enforcement, concerns about confidential data and the need to control their subcontractors (e.g. subcontractors offering data storage/processing services).

Stakeholders identified various benefits from abolishing existing data localisation restrictions. First, and in line with the above, they pointed to cost reductions, specifically more favourable conditions for SMEs and start-ups doing business in Europe. They also argue that stronger competition would correct the existing market distortion (e.g. the wide divergence in server prices in different EU countries). Another advantage of the free movement of data would be improved data security, as providers of a particular cloud service could make immediate safety updates that would benefit users, regardless of their location. Finally, respondents believe that by removing data localisation, the EU would send a strong signal to the international community, encouraging the free movement of data worldwide.

The consultation also provided the state of play of cross-border data activities. Slightly over half of respondents already store and/or process data in multiple locations across the EU. A sector-specific analysis shows that cross-border data processing and storage is much higher in financial services and lower in the public sector, whereas the figures for IT firms and manufacturing are similar to the overall average. In response to the question of why respondents process and store data in multiple EU countries, the most common answer is 'general operational reasons'. Some customers, predominantly of IT services such as cloud computing, demand that their data be stored and processed locally. The main reasons for this are uncertainty about the legality of storing data abroad, perceptions of data localisation restrictions, or unfamiliarity with current EU rules.

As regards the most appropriate measure that could be taken to tackle data localisation restrictions, a legislative instrument received most support, followed by guidance on data storage/processing within the

EU and making restrictions more transparent. Other options were significantly less popular. A number of respondents said it would be appropriate to combine a legislative instrument with a transparency regime for the existing restrictions on data localisation.

In addition to the online consultation, the Commission held three structured dialogues with the EU countries to discuss current data localisation requirements and the reasons for them, as well as issues that may need to be addressed before implementing the principle of the free flow of data principle (such as data security and the availability of data for regulatory purposes). Bilateral meetings were also held with various EU countries. The structured dialogues revealed a general consensus on the need for the free flow of data within the EU if Europe is to be transformed into a data economy. The first such dialogue focused on identifying key benefits of and challenges to data mobility within the EU.

The key benefits and opportunities identified were:

- Economic growth;
- Higher level of competition and innovation in the EU;
- Better "cross-border" use of public sector services;
- Promote and advance legal clarity in the EU.

The key challenges and threats were:

- Lack of mutual trust;
- Legal uncertainty about the applicable rules.

These findings closely match the conclusions of the online public consultation, which also raised the challenges of legal uncertainty and lack of trust.

The second structured dialogue was an opportunity to discuss the current EU legal frameworks for free movement of data and to further elaborate on the data localisation measures identified so far in that context. In general, participants found it very difficult to navigate through all existing legal instruments. Some participants mentioned that the data localisation restrictions identified in their country lacked legal clarity and that their objective was not clearly stated, which makes the proportionality test difficult. This adds to the contention that legal uncertainty is a key driver of problematic restrictions on data localisation.

Of the 112 position papers submitted in response to the public consultation, almost all addressing data localisation called on the Commission to propose a regulation enshrining in law the free flow of data and thereby removing legal uncertainty.

Access to and re-use of data

Comparing the consultation results with earlier evidence[3], companies appear to engage in more data sharing. More than half of respondents indicate some form of dependency on data produced by others. Three quarters of respondents share their data to some extent. Most 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 reuse conditions or against payment of a licence fee.

When asked about obstacles to data sharing, just over half of respondents report no difficulties in obtaining data from other businesses. However, almost half of companies using data say they have experienced some problems in accessing data held by others. Around a third of respondents think neither competition law nor legislation on unfair contract terms or unfair commercial practices fully addresses such problems. Concerns

[3] Cf. Staff Working Document SWD(2017)2 accompanying the Communication 'Building a European Data Economy', COM(2017)9, p. 14.

about fair access to data resources appear to be particularly strong in the automotive after-sales market. Large businesses, however, think competition law tackles problems of abuse of dominant position adequately.

Data holders feel that their investments in data collection (capabilities) are well protected, notably through the Database and Trade Secrets Protection Directives, requiring no additional regulation.

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

However, most stakeholders call for prudence when it comes to any action the Commission might take to make more data available for reuse.

They argue that data value chains and business models building on data are extremely varied, making it difficult to design one-size-fits-all solutions. This view was also widely shared by the Member States represented at a dedicated workshop. Almost all companies or business organisations think freedom of contract should prevail. This would be instrumental so that individual solutions adapt to the concrete needs of a business case. Contracts would build on trust, which is indispensable when sharing data. One aspect of building trust is transparency on how the data will be stored, processed and for what purposes they will be used. Data holders also need to be sure that their business partner complies with data protection legislation and meets adequate cybersecurity standards. Finally, businesses need to ensure that investments in data collection capabilities (in particular sensor-equipped, connected Internet of Things machines, tools or devices) can be recouped, and they need to protect commercially sensitive information.

Many stakeholders commented at meetings and workshops that the crucial question in B2B data sharing was not so much which entity has an 'ownership title' of some sort on the data, but how access is organised. A paper from the European Political Strategy Centre and input received from academia was strongly supportive of this view. Both argued that there was a policy choice to be made between working towards creating property rights on data and working to open up data access further.

The idea of a right to licence data from sensor-equipped machines, tools or devices is thus viewed with scepticism when awarded exclusively to either the Original Equipment Manufacturer (OEM) or the user of a sensor-equipped machine, tool or device. Stakeholders think it unlikely to achieve its stated goal of facilitating the tradability of data by reinforcing its legal status. This potential way forward would on the contrary strengthen the de facto holder's control over access to data, create legal uncertainty in the practical application and thus generate additional legal transaction costs. On the other hand, the idea of an exploitation right to license data use shared among the OEM and the user of a sensor-equipped machine, tool or device, was seen relatively favourable. Representatives of SMEs, in particular, support such a solution.

In general, respondents took a fairly favourable view of an obligation on data holders to license certain data under fair, reasonable and non-discriminatory (FRAND) terms. On the other hand, a third of respondents — especially data-holding companies — voiced strong concerns about this solution.

The 'technical' way forward, i.e. encouraging the use of application programming interfaces (APIs) received most support. As a significant number of respondents remarked, however, APIs are only a vehicle for data sharing and are used when data-holding companies have already decided to share data.

About half of respondents (over or just under 50 %) supported the other proposed ways forward listed in the online questionnaire (guidance on EU legislation, default contract rules paired with recommended standard terms of contract). Some level of support for soft measures such as model contract terms in order to keep transaction costs for smaller participants lower emerged at the workshop dedicated to SMEs. EC guidance on access to and sharing of data received considerable support during the workshop on the data economy at the 2017 Digital Assembly. These solutions are regarded sceptically by a number of respondents, because they are not effective enough for some, whereas they go too far in the view of others. In particular, default

but non-mandatory contract rules for B2B situations paired with an unfairness control mechanism has seen a divided, equal response between those supporting this solution and those disagreeing with it.

In terms of sector-specific situations, participants in both the Digital Assembly and the workshop for SMEs supported the idea of creating testing environments.

Calls for market intervention were strongest with respect to access to in-vehicle data and data generated in a smart farming environment:

- As regards access to in-vehicle data, stakeholder positions are quite pronounced. OEMs cite several reasons why third parties must be obliged to access data through an external server, rather than directly from the vehicle. The main ones have to do with the safety and security of the car. Stakeholders from the after-sales market (including but not limited to the automotive aftermarket) are deeply concerned about the continued viability of current business models and about opportunities for developing entirely new business models. At the workshops dedicated to SMEs and to Smart Industry, this sector strongly advocated regulatory intervention.

- In the agricultural sector, 77 % of participants in a workshop held by the agricultural European Innovation Partnership (EIP-AGRI) thought the data producer (the farmer, the food company, etc.) should have the right to determine who had access to the data produced.

Businesses in the service and repair sector fear disruption as a result of commercialisation of Internet of Things-enabled industrial and household appliances. In their view, OEMs may be tempted to readjust service agreements as a result of superior knowledge of clients' needs resulting from data feedback from such appliances.

The idea of allowing access to data held by companies for public authorities, for public policy purposes, was also viewed relatively favourably, especially as regards reuse for clearly defined purposes (public health risk prevention, access by statistical offices or for publicly funded scientific research). A third of respondents, however, disagreed entirely. Many companies argued that such data access should be fairly compensated, taking into account the investment in data collection or adaptation that would be necessary before the data could be used by public authorities (e.g. converting data into relevant formats, anonymising personal data or confidential business information).

Liability

This section sought to collect information on extra-contractual and contractual liability challenges in the context of Internet of Things (IoT) products and services, autonomous systems and advanced robotics. While several engagement tools were used (studies, workshops, online public consultation), further consultations are considered necessary.

While there is generally limited enthusiasm for changing the current liability regime, a few stakeholders, mainly on the consumer side, regard an overhaul as beneficial and necessary.

The vast majority of producers taking part in the consultation were not aware of any specific problems, nor had they experienced any difficulties as regards liability in the context of IoT products and services, autonomous systems and advanced robotics. Very few had encountered problems with the classification of IoT products and services, autonomous systems and advanced robotics as products or services, or had experienced any significant problems in this area.

Very few of the consumers taking part had suffered damage. The main issues mentioned in position papers sent in by consumer organisations and law firms are the difficulty, as a consumer, of proving that a product is defective, establishing a causal link between defect and damage, and being forced to apply a narrow definition of damage. These papers also highlight the problem of proving that software does not provide the safety consumers are entitled to expect.

Regarding the types of damage suffered that are not covered by the current Product Liability Directive, very few respondents listed 'missed opportunity losses' or 'pure economic losses'. Due to the limited number of responses, there was no clear evidence about the typical amount of loss.

Overall, damage in the context of IoT products and services, autonomous systems and advanced robotics seems to be very rare. This could be because IoT products and services are new to consumers and have low market penetration.

Given respondents' limited experience with actual cases of damage in the context of IoT products and services, autonomous systems and advanced robotics, no clear picture emerges of who should be held liable when such products and services prove defective. Equal numbers of respondents support joint liability of all parties contributing to a product, individual liability of each component producer or liability of the end producer/system integrator.

Some consumer associations stated that since it could be extremely difficult for end customers to identify the component of a smart device that had malfunctioned, they should be able to send their compensation claims to end producers. Some respondents called for new risk management schemes to maximise overall benefits to society and minimise total costs.

Opinion on the preferred liability regime is divided. Some respondents said that liability in the context of IoT products and services, autonomous systems and advanced robotics could be dealt with adequately through contracts, with an equal number taking the opposite view. Many more thought contractual solutions addressed the issue at least in part. Of the 50 position papers that discussed liability, 32 stated that the current liability framework is adequate to deal with the challenges of new technologies such as IoT and autonomous systems. Eight called for the current framework to be revised, and the rest discussed liability without concluding that revision was needed.

Several further findings from other workshops and studies were put forward:

- It is harder (and maybe less meaningful) to draw a line between services and products where technologies such as IoT, autonomous systems and advanced robots are concerned. This makes it difficult to interpret and apply legislation, especially as there is EU legislation on product liability, but not on service liability. For instance, it is unclear to what extent software or digital data (considered separately from a material carrier) can be considered a 'product' across the EU, or how to assess complex offerings with both product and software components, potentially from different manufacturers.
- Another issue is related to the concepts of defect and safety of products, traditionally tied to the safety expectations by the user. The more done to ensure safety, the fewer performance or functional problems are likely to arise during the product's lifetime. How should this be assessed in the cases of autonomous systems and advanced robots, where a product (or a service associated with a product) begins to behave in an unpredictable, potentially risky manner? Nowadays, the issue of safety also involves the changing role of users of products and services, who now help maintain and develop systems by such means as updating software or 'training' products and applications. The Radio Equipment Directive addresses issues related to innovation challenges to do with interconnectivity and the interoperability of products or systems.
- Where composite, complex technologies combining products and services are concerned, it may be difficult to assign liability in the event of damage (i.e. to prove the existence of a defect and the link between damage and defect). In the context of robotics and IoT, this complexity may undermine consumer protection.
- It must also be recognised that complementary laws exist that affect liability issues in a particular ecosystem, such as laws on drones or traffic rules for self-driving cars. This can lead to a fragmentation of liability approaches across EU countries.

The results of sectorial stakeholder engagement in the automotive, businesses services, food and drink supply chain, mechanical engineering and medical devices sector showed that the vast majority of stakeholders (39 of the 40 associations participating, and 6 of the 9 businesses) thought the current liability framework adequate for dealing with emerging technologies such as IoT products and services, autonomous systems and advanced robotics.

While the importance of liability issues is acknowledged, progress in individual EU countries is very uneven. Their main message was that any European-level initiative would need to be discussed further and considered carefully before envisaging any change to the existing legislative framework. Further analysis of the situation should be prioritised, as should supporting innovative businesses which have already encountered these emerging barriers as legal uncertainty, sometimes through legal guidance and legal clarification. Moreover, some EU countries have encouraged the EC to think beyond the policy silos of sector-specific policies — as was done with connected cars — and consider the question of liability as a cross-cutting issue.

Portability of non-personal data, interoperability, standards

Portability

About a quarter of respondents taking part in the online public consultation said they were dissatisfied with the conditions under which they can port data. About a third of respondents claim to have experienced difficulties with porting data. However, looking at the responses received from SMEs, the picture changes. Most SME respondents who intended to switch cloud service providers reported difficulties in doing so. Most cited the option of porting non-personal data as an important factor. Overall, respondents of every category agree that steps should be taken to facilitate the portability of non-personal data. They predict that this will be an issue in the future.

As regards the possibility of the Commission's introducing principle-based rights to data portability in the context of switching cloud provider, many respondents take a positive view, including those from industrial sectors such as transport, energy and utilities. Respondents from the financial sector and academia were cautiously positive. Certain countries, including France and Estonia, have shown interest in introducing legal rights to portability.

Stakeholders from the cloud community also shared their opinions at a workshop on switching between cloud services providers. The main technical challenges cited were a lack of standardisation for application portability, data format challenges, difficulties in identifying/exporting data and metadata, and the estimated time needed for data acquisition and transfer. The main legal barriers cited were data protection concerns, the lack of exit plans and data retention time. The economic aspects are also of concern to cloud users, who often bear the entire cost of switching cloud service provider. The participants were generally positive towards the introduction of an EU legal right. In addition, they mentioned the possibility of developing industry codes of conduct and working to ensure the transparency of APIs.

On the introduction of general (i.e. not cloud-specific) portability rights, many suggest first observing how the right introduced in Article 20 of the GDPR is applied in practice. Many respondents refer to the difficulty in separating non-personal data from personal data. In response to this more general right, many respondents from large companies and organisations say the implementation of data portability is best left to the contractual or technical solutions and industry-led work on standards, as well as skills development for start-ups and SMEs.

Many respondents concentrated on the Business-to-Consumer (B2C) aspects of data portability, although the Communication on Building a European Data Economy clearly focuses on B2B aspects. This may be explained by the prevailing consumer/data subject focus of the public debate around portability issues.

Moreover, attitudes toward data portability may vary from sector to sector. Participants in the April 2017 agricultural workshop said data portability should be an essential and free-of-cost feature of any platform, enabling producers to transfer their data to competing or different platforms.

Interoperability and standards

Interoperability is a pressing issue for many of the respondents to the online public consultation, and there is a consensus on the need for interoperability standards.

Most cloud user respondents prefer standard-compliant solutions, and generally also open standards. Numerous examples were given of standards relevant to cloud computing, including standards on access, data formats, cloud security, data protection and APIs. The main reasons for requesting standard-compliant solutions are security, data and privacy protection.

Among technical measures to facilitate data access and discoverability, common metadata schemes were most prioritised. More respondents would prefer an improvement of existing standards, rather than defining new ones, but many also welcome recommendations to implement their priorities. Where legal instruments are concerned, most respondents opt for guidelines, followed by EU regulation and support actions.

Judging from comments on open sections in the questionnaire and from the position papers received, many think it should be left to industry to develop standards, or that the Commission should look at existing work on standards (both cross-cutting and sector-specific) before taking any further measures. Many respondents prefer technical solutions to data economy issues, rather than legal or policy solutions. Results from sectorial stakeholder engagement confirm this.