Minutes of the consultation Workshop on the Free Flow of Data initiative

18 May 2016, 10h00 – 17h00, BU25, Brussels, Belgium

SUMMARY

The European Commission explained the context and objectives of the Free Flow of Data (FFoD) Initiative under the Digital Single Market (DSM) Strategy, presented an overview on the most important issues to be addressed by the FFoD and emphasized the importance of an evidence based law-making characterized by studies, public consultations and stakeholders input.

The essential objectives of the FFoD initiative are, on the one hand, the abolition of unjustified data location restrictions and, on the other hand, addressing other factors inhibiting or preventing the FFoD in Europe, labelled as "emerging issues". The latter emphasis comprises the ownership of data, access to data and its re-use, as well as liability, interoperability and portability.

The Commission provided an overview on the most important input and evidence gathered up to this point of time. First, reference was made to the public consultation on platforms and the recently published synopsis report summarising the responses received, which suggested that action with regards to data location restrictions is needed. In relation to the emerging issues, however, while the current contractual framework was considered not to be fit for purpose, the were divergent opinion son what steps needed to be taken. Second, two studies on data location restrictions were presented, planned studies briefly addressed and relevant workshops and conferences in the past as well as future mentioned. Furthermore, potential options for action as supported by the input and evidence gathered were briefly touched upon.

The discussion on the first issue demonstrated clear support for the abolition of unjustified data location restrictions in the light of technological developments and costs. In relation to access and ownership of data, a clear divide could be observed and scepticism in relation to potential regulation was expressed even though most participants confirmed that access to data must somehow be granted. In relation to liability it was generally acknowledged that the current regime needs to be adapted to emerging technologies and future challenges, whereas with regards to interoperability and portability caution with regards to premature standardisation was expressed. In conclusion, cost and a lack of trust were identified as two critical considerations framing the FFoD discussion.

1. WELCOME AND INTRODUCTION

Pearse O'Donohue (Head of Unit "Software and Services, Cloud" - **POD**) opened the meeting and welcomed the participants. He recalled that the Commission had put an ambitious agenda on the table in the Digital Single Market Strategy published in May 2015. He pointed out the importance of a common market for digital services and products in the context of the DSM Strategy. He thanked participants for their attendance and introduced the agenda for the day. He invited the participants to provide input and to raise any issues faced by the industry along the consultation workshop.

2. THE FREE FLOW OF DATA INITIATIVE IN THE CONTEXT OF THE DIGITAL SINGLE MARKET STRATEGY

At the outset POD identified the Free Flow of Data initiative as third main objective, besides the European Cloud Initiative and the Interoperability and standardisation efforts engaged in, of the roadmap to enhance the Digital Economy in terms of ensuring development and use of data, data technologies and services (e.g. cloud computing, IoT, big data) across all sectors of the economy.

POD outlined the four recent communications by the European Commission adopted on 19 April 2016 in relation to the Digital Single Market (DSM) and public sector modernisation, such as the chapeau communication on Digitising European Industry, the European Cloud initiative, the Priorities for ICT Standardisation and the Egovernment action plan 2016-2020.

In relation to the Free Flow of Data initiative POD pointed out its two-fold emphasis. On the one hand data location restrictions on data are being targeted and, on the other hand other factors inhibiting or preventing the flow of data will be considered. The latter factors being labelled as 'emerging issues' include issues, such as 'ownership', access and re-use of data, interoperability and data portability, as well as liability. The impact of these barriers must be assessed and based on collected evidence potential measures will be identified. For this purpose the European Commission launched the public consultation on Platforms, gathers data and inputs in order to shape the impact assessment. The Synopsis report on the contributions to the public consultation on the regulatory environment for data and cloud computing[1] published on the 12 May 2016 reflects some findings and today's Consultation Workshop bring further input and evidence.

3. PLANNING AND PREPARATION OF THE FREE FLOW OF DATA INITIATIVE

3.1. LATEST REPORTS

Vanessa Vanwesemael (DG CONNECT – VVw) provided an overview of the public consultation on platforms, which contained a specific section on data and cloud, and made a reference to the summary report as well as the synopsis report on data and cloud published thereof. After outlining the most important figures of the public consultation and identifying the types of respondents as well as the geographical distribution, the main findings presented by VVw were:

First, the public consultation confirmed that data location restrictions are affecting the use of data services and business strategies. Further, they can act as a barrier to the development of the data economy and the competitiveness of industry in Europe and there is a need for action. However, it was also established that there are nevertheless justifiable grounds for some data location restrictions, under strict rules (e.g. national and public security).

Second, in relation to data access and transfer the public consultation has shown that the current legal framework (n.b. for contracts) appears to not be fit for purpose and citizens as well as consumer groups support the need for legal clarity. On the other hand, many service providers share the view that the current framework suffices. They stress the importance of contractual freedom as regards 'ownership' and tend to favour soft measures. Additionally, some respondents indicated difficulties in distinguishing between personal and non-personal data, but there could no clear consensus be detected on the measures to take for non-personal data generated by a device in an automated manner.

Third, in the context of data markets it was found that the perception of data as an economic asset is crucial for competitiveness of the EU. However, a number of issues are being perceived as regulatory constraints holding back the development of the data markets (e.g. trust and privacy concerns, data localisation requirements). Therefore, further EU efforts facilitating access and re-use of non-personal data were encouraged. This confirmed that there is a need of legal certainty in order to stimulate investment.

[1] https://ec.europa.eu/digital-single-market/en/news/synopsis-report-contributions-public-consultation-regulatory-environment-data-and-cloud

3.2. INPUTS AND PLANNED STUDIES

Judit Schveger (DG CONNECT - **JSc**) introduced the two ongoing studies on data location restrictions. One of them is an Exploratory study mapping data location restrictions in 8 Member States executed by London Economics/CARSA on the one hand, and a Comprehensive study mapping data location restrictions in all 28 Member States and quantifying their impact (economic analysis) on the functioning of the internal market conducted by SPARKS/Timelex/Tech4i2 on the other hand. JSc emphasized the importance of both studies for the steering of the European Commission's understanding and as a consequence directly impacting the impact assessment on the Free Flow of Data initiative.

Furthermore, JSc mentioned the Study on the European Data Market by IDC & Open Evidence, which identified current and future trends on the European Data Market, thus also addressed the key emerging issues of data ownership and access to data. Additionally JSc made a reference to the highly relevant panel discussion on the free flow of data and especially the emerging issues of data ownership and access to data at the Netfutures 2016 conference on April 22nd 2016. The Industry round table also organised by DG CNECT on the 'Free flow of data: Emerging issues of "data ownership"' in Luxembourg which took place on the 17th March 2016 was also referred to.

In conclusion, JSc briefly introduced a recently launched Impact Assessment Support Study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability. This study ought to particularly focus on current business models, contractual terms or commercial practices as part of the data value chain. Preliminary results would be expected in 8 weeks after the signature of the contract. Furthermore, a study on portability will also be launched soon.

3.3. OPTIONS

POD outlined the identified main problem in the context of the preparation on the impact assessment, which is the curtailment of the DSM and the growth potential of the digital economy without a free movement of data across the EU. Data must flow freely and smoothly within the EU in order to exploit the full benefits as well as potentials of data technologies and services. Data location restrictions and other factors inhibiting or preventing the flow of data, such as uncertainties with regard to 'ownership', access and re-use of data; interoperability and data portability; liability arising from the use of data, and liability in relation to IoT products and services also have strong implications to the Free Flow of Data.

POD highlighted the lack of clarity and predictability of applicable rules; different national and sectorial rules/practices fragmenting the market; the high costs of entry to the market and costs to implement new technologies and the complexity of current framework and its non-appropriateness for fast evolving technologies as being only some effects caused by the issues identified.

In view of the Free Flow of Data Impact Assessment alternative policy options are being explored, without prejudice to the final decision of the Commission. POD identified the improvement of existing legislation or the creation of a new one; a soft-law approach in terms of a recommendation or communication; and a mixed approach as opposed to a common approach to be the various alternatives for measures addressing data location restrictions and

emerging issues. Currently an impact analysis and a comparison of options (including the status quo) are being analysed diligently.

In the light of the impact analysis POD underlined the importance of consultations for gathering the view of the industry and presented the consultation plan for the future, which includes dedicated workshops with Member States representatives and further required stakeholder workshops. The next two scheduled workshops will be the Workshop on the Data Market on the 28th of June in Eindhoven and a Seminar with Commissioner Oettinger in September.

3.4. Discussion

Generally a strong support for the Free Flow of Data initiative was expressed by the participants of the consultation workshop and it was confirmed that the scope of the initiative by the European Commission captured almost all relevant issues. However, it was mentioned that a reference to Intellectual Property Law as well as Competition Law would be desirable.

Further, required authorisation through MS for cross-border operation and set-up of IoT applications as well as services was identified to be another potential barrier to a common digital market. Due to the high relevance of the IoT service market for the industry and the critical roles of data for such services, any curtailment to the free flow of data would have a negative impact on the economy.

In relation to the differentiation between personal and non-personal data it was made clear once again that there is a clear framework covering the former, thus no interference with this framework is neither intended nor needed. Hereto Anna Pouliou (GE – AP) emphasized the role of pseudonimisation and the difficulty to determine non-personal data in terms of a lack of clarity by the GPDR with regards to pseudonomisation and anonymisation of data. AP made a reference to an internal study which identified 30 grades of anonymity of data ranging from highly sensitive personal data to irreversibly and fully pseudonymized and anonymized data. A follow-up on pseudonomisation could be helpful before addressing data location restrictions.

Paul Foley (Tech4i2 - PF) pointed out that a current study for DG CNECT on the social and economic impact of 5G has shown that in order to reduce congestion, access on data is needed. Thus not only the question as to the ownership is highly relevant, but especially the information on whether data is personal or non-personal. POD referred to legislation already in existence for the public sector.

Rainer Koch (German Telecom – RK) confirmed the importance of anonymisation in the context of traffic management and especially in relation to trust in smart city projects. However, the freedom of contract is highly important for B2B and the right balance must be upheld.

For the automotive sector the essentiality of the distinction between industrial data and personal data was underlined. There is a high risk of potential bottlenecks on data through control and blockage by major industry players. On the one hand, for personal data consent and portability are obligatory, but on the other hand, no portability for industrial data is given. On top of that other legal regimes, such as the competition law and trade secret law complicate the matter. In order to enable fair competition and a level playing field, there might be need for mandating access.

With regards to the geographical scope of the Free Flow of Data initiative it was confirmed by the German Telecom that the GDPR and the NISD already create an equal playing field beyond Europe, thus within the EU the Free Flow of Data initiative is a good starting point.

4. DATA LOCATION RESTRICTIONS

4.1. Presentation of the preliminary results of the study "Facilitating Cross Border Data Flow in the Digital Single Market" conducted by CARSA and LE Europe

Moritz Godel (London Economics – MG) provided an overview on the background on the issue of scale and the investigation of technological, technical and legal barriers. MG identified the objective to be the understanding of the restrictions and the need to focus on both, legal compliance and soft restrictions. Restrictions can be explicit or implicit. Further, user preferences were also considered and the study has shown so far, that there is a wrong perception of relative security when keeping data in the local jurisdiction. In the context of the study several companies in 8 countries expected to be subject to restrictions were interviewed and an online survey was launched. MG provided some sectorial examples in some of the MS and elaborated on the perception of the legal restrictions.

4.2. Presentation of the preliminary results of the study " Cross border data flow in the digital single market: study on data location restrictions" conducted by time.lex, Spark and tech4i2

Patricia Ypma (Spark – PY) presented the study objectives, which were the identification of legal and non-legal barriers and the quantification of their impact. The study was aligned with the study "Facilitating Cross Border Data Flow in the Digital Single Market" conducted by CARSA and LE Europe. Furthermore, the methodology of the study is comprised by a survey as well as interviews, a cost-benefit analysis and recommendations. The first results on compliance obligations were based on various sectorial investigations and distinguished between direct barriers in terms of direct legal obligations and indirect barriers, such as the accessibility to data by authorities/regulators and implicit data retention obligations. The barriers in the financial and the health sector have shown to be predominantly indirect.

4.3. Other short presentations

Julien Debussche (Bird & Bird – JD) briefly outlined the legal barriers to the free flow of data in terms of both, personal as well as non-personal data. Further JD identified potential legal issues for personal data, impacted sectors and impacted technologies. In relation to non-personal data a number of legal areas impacting the free flow of data were identified, such as ownership and IPRs, security, tax/accounting, liability, trade secrets, Competition.

Christian Borggreen (CCIA – CB) emphasized that companies increasingly file and store their data online and referred hereto to a study commissioned by CCIA, which has shown that EU Member States often have conflicting rules on: Location, format and length of allowed data storage; Legal, audit and financial reporting requirements; and rules for companies use of cloud technologies. CB concluded that a patchwork of national rules on company data disincentives for firms to utilise the EU Single Market and especially hits SMEs disproportionately hard. In relation to the FFD CB described it as a historic opportunity to simplify company data barriers, which fragment the EU Single Market and stop businesses becoming “European”.

William Echikson (E+Europe – WE) provided an insight on the cost-benefit considerations as well as other selective criteria for investors in the context of the establishment of data centres in Europe. Some of the criteria identified were cost of land, water and energy as well as legal obligations and the costs thereof. Based on the example of some MS WE illustrated why most investment goes to Frankfurt and the UK. In his work with ECIPE costs of restrictions and of misleading investment are being quantified.

Yen-Ming Chen (Microsoft – YMC) identified residency requirements and especially requirements dictated by perceptions rather than by law to constitute selective criteria. The two main drivers for Microsoft current data centre in Germany are sovereignty and residency requirements since customers demand data to be in their own MS in order to avoid access through national security agencies. Some MS align with this sentiment, such as France where for a basic cloud label guaranteeing a basic level of protection, data must be stored in the EU, whereas for a stronger level of protection guarantee the data must be stored in France. This does contradict the generally agreed fact, that a free flow of data would increase security and privacy risks.

4.4. Morning discussion

POD emphasized that the work is in progress and no final decision as to the scope was reached. Even though the presentation gave an idea on the scope, the European Commission calls for action in terms of providing input. The costs to companies by data location restrictions and other barriers which as a consequence pass on to customers and the impact on the whole EU economy are of special interest to the European Commission. Further, it appears that the lack of information and wrong perception with regards to barriers constitutes another considerable issue, which has to be addressed since it was proven that storing data on premise is less secure than migrating to the cloud. However, mass surveillance has strongly influenced perceptions and affected trust. A clarification on the trust for enterprises and customers would be helpful according to Michael Symonds (Atos – MS).

In relation to the Free Flow of Data the view was supported that a reverse burden of proof is needed, which requires MS to justify data localisation restrictions before imposing them. This would be especially reduce cost in terms of data processing, which would otherwise increase costs drastically if subjected to exaggerated data location restrictions.

Furthermore, POD confirmed the EC's endeavours on certification and standardisation in order to facilitate data and network security among others. Carsten Kestermann (Amazon – CK) added that different terminology and interpretation despite very similar technologies within the EU often is a result of convenience rather than real restrictions in relation to security standards. Additionally it was underlined that security and liability questions constitute costly issues for users.

POD called for input on individual examples of data location restrictions and identified the elements of trust and the costs as being the most selective criteria for cross-border data flows.

4.5. Afternoon discussion

JSc provided a follow-up on the morning presentations and discussion in terms of the European Commission's definition of data location restrictions; drivers and consequences; the scoping including the distinction between personal and non-personal data; as well the question as to whether address only EU level or also global level.

In view of data location restrictions POD initiated a discussion on justified and legitimate restrictions on the Free Flow of Data imposed by MS. The most obvious examples, such as criminal records, patient rights in relation to health data and cases were the sovereignty of MS are affected were generally acknowledged. However, situations in which supervisory powers and regulatory checks needed to be exercised, such as for example in the financial sector, it was questioned whether accessibility requires retention within the territory of a MS. In relation to this point, a reference was made to FISMA according to which financial regulators need immediate access. The European Banking Federation suggested in the light of ongoing studies that a global dimension would be of added value in terms of enabling competitiveness.

Moreover, RK (German Telecom) pointed out that the NIS Directive is already outdated in terms of an insufficient scope and unsuitability for new technological developments, such as is also the case for the Data Retention Directive. RK urged for respecting customers choices in relation to trust motivations. Furthermore, language and proximity were identified as being two main motivations for user choices by SMEs. However, it was also made clear that for some technologies, such as block-chain and distributed layer which do not work on a single data set, but use multiple copies on multiple machines, data location is completely irrelevant. This was confirmed by Nokia in relation to virtualisation and network technologies. Another point raised was the need for assurance for sustainable encryption and the assurance for destructions of data according to user preference or legal obligation. In relation to this also the question as to at what stage MS will request the keys.

In conclusion it was again confirmed that the first concern is the cost base for users as well as for providers and that the cost of breaches in the context of differentiating between personal and non-personal through anonymisation/pseudonomisation of data might lead to high levels of unpredictability.

5. OTHER BARRIERS AND EMERGING ISSUES

JSc briefly recapped the emerging issues of ownership, access and re-use and made a reference to the related workshop organised by CNECT.G3 last March. Furthermore, the liability issue and the question as to who is to blame in the supply chain were raised. Interoperability and portability of data were also identified as other barriers.

Patrice Chazerand (Digital Europe – PC) presented a brief position paper on the concept of ownership, which identified data as new currency and rejected a uniform answer. All B2B and B2C contexts are different and suitable legal frameworks already exist, such as contract law, IP and database rights, competition law, trade secrets, consumer protection and the GDPR. Digital Europe expressed to be in favour of the freedom of contract since no equal claim to all data could be established and no evidence is given that contractual negotiation is not working.

Further, it was generally acknowledged that there must be reconciliation between business providers and public objectives. Some argued that currently privacy and data protection considerations outweigh profits as well as business interests in Europe.

Javier Villegas-Burgos (Vodafone – JVB) emphasized that the transition to the IoT will require a move away from bilateral contracts towards multilateral contracts and therefore time is needed

to assess whether the current legal framework suffices in relation to ownership of data. Telcos are aware of the fact, that they will never own the data. However, in relation to use cases such as connected cars, the issue of data ownership must be assessed diligently. If some market players have control most or all of the data, it will affect the value chain and in the worst case have a chilling effect on the IoT.

Moreover, the right to exclude inherent in the concept of ownership was critically questioned in the context of a digital world. Instinctive reactions pointed towards a permission concept instead. In relation to this model contracts with implied contract terms were mentioned as a potential solution. However, the valuation of data is perceived as a contrasting and difficult issue, and some argued that data loses value as soon as it is created and is outdated very quickly (e.g. Wearable devices). In the light of these points raised the question as to who has the right to grant permission was emphasized.

In relation to liability and the question of accountability for faulty technologies and bad data quality, simplicity is sought for, but complexity is given. Especially, when it comes to the IoT one faces a hybrid situation of 2 existing legal frameworks consisting of the Product Liability Directive and the Services Directive and is challenged by the question as to applicability of either one of them, both or none. The issue gets even more complicated in terms of cognitive decisions by machines and the allocation of liability in terms of algorithmic responsibility. How to incorporate privacy, moral and ethics? Accordingly there must be made a distinction of liability for data and systems. Some push for a more granular approach of liability in the light of its potential merits in distinguishing between economic and non-economic loss. The public sector could take the lead on that, but obviously the question arises whether exposure to liability and consequentially large damages would be desirable for public bodies and if not, how to protect public bodies acting in public interest.

When speaking about interoperability and portability of data, it must be understood that the former is a prerequisite for the latter. This is not only important for users to move their data to other servers, but also for the emergence of greater choice in the context of hybrid cloud and other complex models. Therefore it is necessary to direct efforts towards creating standards by using open source software as guidance. In a complex market interoperability can be addressed by targeting gaps for new technologies needed to make data interoperable.

With regards to specifically portability, Sue Daily (TechUK – SD) observed that data will increase and users will want move data on-demand. Hereto, the portability clause included in the GDPR could facilitate the discussion and progress. However, equally commercial, legal and technical aspects must be considered. One solution could be to give effect a portability right, but in must be kept in mind that it is an issue of managing expectation on portability – not every data can be moved (e.g. metadata). Also demand on the customers/user side can push for interoperability due to the urge to not be locked in. However, it must be avoided to standardize prematurely in light of different architectures, sources, formats etc. At the beginning the demand for more synergies between different solutions must be satisfied. Service Level Agreements could be a first progress towards portability in terms of providing SMEs with the right questions for CSPs (see the outcome of one of the EU funded projects, SLALOM tool).

6. CONCLUSION

POD concluded in confirming an action on behalf of the EC in relation to data location restriction in terms of at least requiring a strict burden of proof for MS when justifying restrictions. The emerging issues will require further scoping and as a consequence contributions and supporting evidence is welcomed. There might be a consultation on the FFD during the C-SIG plenary in the form of a video-conference. Further comments are welcome on the Inception Impact Assessment after its publication.

POD thanked all the participants and closed the plenary meeting at 17h00.

Speakers and Panellists:

- O'DONOHUE, Pearse – European Commission, DG CONNECT, Head of Unit and Chair
- SCHVEGER, Judit – European Commission, DG CONNECT
- VANWESEMAEL, Vanessa – European Commission, DG CONNECT
- GODEL, Moritz, London Economics, Associate Director
- YPMA, Particia, Spark Legal Network, Managing Director
- FOLEY, Paul, Tech4i2 , Director
- ECHIKSON William, E+Europe, Director
- BORGGREEN Christian, CCIA Europe, Director of International Policy
- CHEN Yen-Ming, Microsoft, Principal PM Manager
- DEBUSSCHE Julien, Bird&Bird, Associate