Ref. Ares(2017)1248292 - 09/03/2017

Outcome of the workshop

Workshop `Facilitating cross border data flow in Europe – on data location restrictions`

26 February 2015 - European Commission, Avenue de Beaulieu 25, 1160 Brussels

Participants:

Pearse O'Donohue	EC, CONNECT.E2, Head of Unit Software & Services, Cloud
Francisco Medeiros	EC, CONNECT.E2, Deputy Head of Unit Software & Services, Cloud
Dirk Van Rooy	EC, CONNECT.E2 Head of Sector, Software & Services, Cloud
Tjabbe Bos	EC, CONNECT.E2Policy Officer, Software & Services, Cloud
Judit Schveger	EC, CONNECT.E2 Legal Assistant, Software & Services, Cloud
Fernando Tessoro-Carratero	EC, CONNECT.H4 Project Officer, Trust and Security
Hans Graux	Time.Lex, Rapporteur/Facilitator to the ECP Steering Board
Isabell Conrad	SSW Schneider Schiffer Weihermüller, Germany, Legal expert
Sam De Silva	Penningtons, UK, Legal expert
Paolo Grassia	HP
Eric Henault	EuroCIO
Nicholas Hodac	IBM
Jonathan Sage	IBM
Luukas Kristjan Ilves	Permanent Representation of Estonia
Danielle Jacobs	INTUG
Morten Jorsum	Danish Agency of Digitisation
Evert Koning	De Nederlandsche Bank, Head of Department of Operational Risk and Data Quality
Mark Lange	Microsoft
Corinna Schulze	SAP
Michael Symonds	ATOS
Bartłomiej Trętowski	Council of Bars and Law Societies, Polish Bar Association

In the March 2014 Trusted Cloud Europe report, the European Cloud Partnership's Steering Board noted that "Member States' practices and in some instances national laws restrict the possibility of storage and processing of certain data (especially public sector data) outside their territory". In the July 2014 Data-driven economy Communication (COM(2014) 442) the Commission acknowledged that "data location requirements limit the cross-border flow of information and form a barrier to a single market for cloud computing and big data". Data location requirements can be harmful as they limited the extent to which economies of scale can be achieved, which might in turn obstruct the development of a Digital Single Market as regards data technologies and services.

The Commission committed to study such barriers and to consider future policy actions, notably by taking into account the Trusted Cloud Europe report.

The aim of this workshop is to have a preliminary exploration of concrete examples of data location requirements that limit a single market for cloud computing. The workshop is organised with the intention to trigger a discussion and get a better understanding of such limitations by identifying and collecting real-life examples on existing barriers to the free flow of data within the European Union. Concrete examples will help the European Commission to identify and understand if and where these restrictions exist and what their impact is.

In the workshop several examples of cloud data location requirements were mentioned by the participants that form barriers to the use of cloud services within the European Union. Nevertheless, it is still unclear what is the scope and magnitude of such barriers in EU member states.

A. Data location requirements

Mainly two types of data location requirements were identified in the workshop from a user perspective: I. compliance obligations set out in legal acts or in administrative requirements on the basis of legal acts; and II. requirements not related to a compliance obligation such as user sentiments.

I. Compliance obligations

Compliance obligations that hinder the cross-border flow of data may either be (I.1) explicit or (I.2) implicit. The former hinder the cross-border flow of data explicitly, stating for example certain types of data should be stored in a specific location (eg. example mentioned in the workshop: according to specific regional legislation tax related data processed by a German company should be stored the country). Usually explicit compliance obligations can be regarded as proxy for security or preservation of professional secrecy. The latter are less clear and appear to implicitly restrict the cross-border flow of data.

These compliance obligations may be found at various levels: legal acts issues by the legislator (I.a) at the Member State or (I.b) lower level regulations (regional, county etc.) (I.c) and / or administrative requirements, policy documents and / or enforcement actions.

I.a. Legal acts at Member State level

I.b. Legal acts at lower level

I.c. Administrative requirements

At a lower level, following lower level regulations and or the interpretation of certain policies, there appear to be several examples of data location requirements. Such policies could also be implicit, as part of the risk assessment exercise for the adoption of cloud solutions. In order to identify such policies, it was suggested that one should have a look at amongst others procurement rules, and might even have to go into further detail as regards lower level regulations. Internal policy documents, guidelines or even decisions or permissions (and preconditions for a positive decision) of relevant authorities were also mentioned as a source of these administrative requirements.

Such administrative requirements might also be based on the interpretation of a specific legal act or on the risk appetite and / or sentiment of the public sector towards cloud services (see also point II. Below).

Data location requirements in relation to health data, financial data and professional secrecy (lawyers and legal professionals, medical professions, social care, clerical professionals, civil servants) were identified in Member States' legislation, for instance in Germany. Data location requirements were also identified in relation to financial data in Luxembourg as well

In case of explicit requirements in Germany, the applicability of legal requirements depends on the actors (public or private bodies), type of sector and types of data. Examples mentioned exist beyond the German general data protection law. Under German law “Data location requirements” can be understood as (1) requirements on the location of the registered office of the CSP or its subcontractors (e.g. registered office must be located in Germany or in a specific German state); (2) requirements on the export of data means the location of the server on which the data are stored (e.g. data may not be transferred or stored outside Germany or the EU/EEA); (3) requirements on IT outsourcing means constrains on the contracted data processing (e.g. data may not be disclosed to a CSP). There are also additional requirements which restrict IT outsourcing to CSPs: such as (a) risk management in the financial sector; (b) minimum storage periods for tax relevant, medical or law firm data); (c) access or control rights of competent data protection authorities.

II. Requirement not related to a compliance obligation'

a. User sentiment/customer requirement

Besides lower level or implicit barriers to the free flow of data in relation to cloud services, some of the barriers mentioned in the workshop are based on the sentiment of the user (e.g. a participant representing a CSP mentioned that they're often approached by (potential) customers with the requirement that costumer data should be stored in a data centre located in one Member State, even though customers cannot refer the legal basis for these requirements.)

Participants agreed that data location requirements are not only a legal problem, because cloud users seek secure solutions, have fears from uncertainty and have concerns about the use of new technologies. It was also mentioned that customer requirements are key for CSPs.

In relation to users' sentiments and non-legislative requirements it was also discussed that cloud users (e.g. financial institutions) often claim that requirements come from the regulator. Since these requirements are only laid down in internal policies or they are in written or unwritten guidelines for a decision maker, it would require an approach that also goes beyond regulatory solutions, taking into account the types of data or the legal justification behind such requirements, .Participants also agreed that misinterpretation of the legislation could often be a reason for 'implicit' data location barriers.

B. Risk assessment

A general approach of cloud users towards the risk analysis of cloud based services was also discussed. Cloud users usually make their own risk analysis in relation to cloud services and depending on their risk appetite; they make decisions on their requirements for the cloud service. Following the assessment, they sometimes use data location requirements as a proxy to mitigate certain risks, such as relating to security. The presentation from a Dutch financial regulator point of view on the importance of a risk assessment was mentioned as a useful example that proves to be more willing to align sector (ie. financial sector) specific requirements.

From a financial regulator point of view, risk assessment is a continuous exercise in order to achieve a specific aim eg. to maintain the stability and integrity of the financial sector. It is not only performed on one specific aspect but on all aspects the auditor thinks are relevant (e.g. including strategy, structure, network and information security, etc). Nevertheless, it was also stressed that the supervision (right to audit) must not block the development, adoption of new technologies.

Risks need to be demonstrably known and they should be mitigated in the risk management plan of the organisation (eg. Exit/switching clauses of a cloud service agreement are also particularly important.)

During the discussion it was also mentioned, data location requirements are linked or might be linked to security requirements. Sensitive information governance rules sometimes indicate, the location of the data will often be a risk factor that may weigh on any decision to export such data (eg. UK).

Natural catastrophes (e.g. earthquakes) are also mentioned as an example where security (i.e. availability) of a service actually benefits from geographical dispersion. In case of such natural disasters, the security (i.e. availability) of cloud services is actually improved with using cloud services without data location requirements. It was also mentioned that data location requirements could be disadvantageous for the performance of the cloud service, such as in relation to latency.

C. Cost of data location

A representative of a CSP provided an example where a dedicated data centre was built in order to satisfy a customer's data location requirements, even though those requirements were not based on formal data location requirements. It was clarified that building a dedicated data centre to meet such requirements is not always necessary from a technological perspective and obliges cloud service providers to make significant investments.

Another participant raised as an issue the costs of data location requirements and highlighted that an adverse effect of data location requirements could be that countries with more liberal policies could lose out as CSPs will choose to locate their facilities in countries with strict data location policies to meet their strict requirements.

D. Necessary/unnecessary restrictions

A possible distinction between necessary and unnecessary restrictions was also mentioned. In the Danish example[1] e.g. restrictions were deemed not to be necessary, because the goal (i.e. to give access to financial information for audit purposes) could have been achieved in a less restrictive way. Nevertheless in some sectors restrictions were deemed to be necessary by some participants. Such a distinction was found to be in line with a risk based approach, and the risk management process also needs to be taken into account.

There was also a discussion on the solution that was found for the Danish example. Some regarded it as a half-way solution because the data still has to be stored in Denmark once a month. It was raised that this means that extra licences for services might have to be acquired, which obviously is a concern from a user's perspective.

Some participants were of the opinion that a decision on the distinction between necessary and unnecessary data location restrictions should be left to the controller of data, but others were of the opinion that this would leave too much room for subjective interpretations.

The mentioned examples are combination of compliance with both legal or non-legal requirements and user sentiment. Nevertheless, it was also stressed that the market is now mature enough, so that these examples are more about complying with specific rules than result of irrational user behaviour. In relation to necessary restrictions, it was also mentioned that sometimes data owners could not afford mistakes so such they tend to opt for stricter rules.

In relation to necessary data location restrictions it was emphasized by one participant that storing top secret data in a country does not necessarily make sense because it could actually be safer to store the data in another country. It was also explained that in the context of national security, export control, and certain categories of data are usually marked as protected information.

E. Public sector

It was also discussed that data location requirements seem to be more prevalent within the public sector than in the private sector. It was mentioned that risk averseness of public sector organisations is generally higher than in the private sector. Besides a different level of risk appetite it was also emphasized that governments are lagging behind and are less mature than private sector organisations. From a CSP point of view, myths and misconceptions might be easier to address for private sector customer, but it is more difficult to find a solution for public sector users.

[1] A specific example of a data location requirement could be found in the (old) Danish Bookkeeping Act and Accountancy Act that prohibited the use of services that stored information in third countries. The relevant provision of Act have since then been addressed in order to allow for the use of cloud services. According to new rules accounting documents can be stored in third countries, if a full copy of the material is downloaded monthly to be placed on a server or in paper form in Denmark.

F. Other Findings

It was raised that several interpretations of what constitutes a data location restriction seem to exist.

It was agreed that a hesitation of users to adopt cloud services is sometimes related to the location of data, but requirements which were set out in legislative acts are not always the root cause for it. Nevertheless, users' concerns are clearly visible and it was found to be necessary to guard against those concerns turning into legislation.

The usability of an EU-wide data classification scheme was also mentioned, which could serve as an assurance for cloud users. But participants agreed guidelines on data requirements could be more helpful, .Such guidelines could give direction to cloud users and CSPs on what data types are subjected to proportionate and justified requirements in one Member State and help users to understand what obligations they really have. In relation to data classification to decide which requirements are necessary it was also explained that national security: export control, and certain categories of data are usually marked as protected information. It might also be necessary to make a better distinction between different types of data (e.g. personal data and non-personal data), in order to define what necessary and unnecessary restrictions are. Nevertheless, it was also mentioned that cloud users actually might not have the necessary knowledge or maturity to identify and define their own data sets. One participant clarified that large enterprises usually know what types of data they're using, but SMEs usually do not.

The notion of vital or critical services was also discussed on the basis of the Estonian example. Definition of vital services obliges vital service providers to ensure the continuity of the vital service in a manner and by using means that do not depend on information systems located abroad. The list of vital sectors in a legislative act might be based on political definition eg. Estonian Emergency Act.

Certification was mentioned as a possible solution for greater transparency for cloud users.as it could serve as an assurance for users that CSPs are compliant with specifications and standards. Additionally, further need for a harmonised European framework was also mentioned by the participants especially to facilitate comparison and assessment of service providers;

Participants also mentioned that the new data protection rules could be helpful in the future as regards personal data and also a risk based approach could solve problems in relation to data location barriers for cloud service adoption. It was mentioned that a Code of Conduct for cloud CSPs could give a good balanced view, because it could support the uniform application of EU personal data protection rules in relation to a specific technology or service model.

It was also suggested that member states could define specific functional needs, similar to the Service Directive eg. i.e. when they are non-discriminatory, justified for reasons of public policy, public security, public health or the protection of the environment and do not go beyond what is necessary in order to achieve their objective. Some participants rose that data location is important from a compliance perspective and might be addressed in a contract.

The Danish example was mentioned as a useful approach how codified legal requirements could be identified. A guideline to promote the adoption of cloud computing for public organisations could include the mapping and merging of standard cloud contracts with national legislation - with special attention to the national data protection legislation and specific legal acts.

In the discussion it was also stressed that it could be the role of the EC to raise awareness and educate cloud users about the meaning of formal or relevant data location requirements. It was raised that users should be educated in order to be able to better use a risk assessment as regards the risks related to the use of cloud services and data location requirements.

G. Summary

Following the workshop it was found that users experience certain barriers to the free cross-border flow of data in relation to eg. cloud computing services.

Such barriers may either exist for reasons of

(A) compliance obligations set out in legal acts or in administrative requirements on the basis of legal acts;

(B) requirements not related to a compliance obligation such user preferences.

Compliance obligations that hinder the cross-border flow of data may either be

(A.1) explicit or

(A.2) implicit.

The former hinder the cross-border flow of data explicitly, stating for example certain types of data should be stored in a specific location (eg. example mentioned in the workshop: according to specific regional legislation tax related data processed by a German company should be stored the country). The latter are less clear and appear to implicitly restrict the cross-border flow of data.

These compliance obligations (A.) may be found at various levels: legal acts issues by the legislator at the Member State or lower level regulations (regional, county etc.) and / or administrative requirements, policy documents and / or enforcement actions.

It was also mentioned in the workshop that certain types of data (eg. health data etc) are well regulated similar to the concept of ‘overriding reasons relating to the public interest’ in the Service Directive. In order to understand the same notion in relation to the free flow of data, the classification of data requirements in Member States might be useful as well.

Requirements not related to a compliance obligation such as user preferences (B) may sometimes be based on misconceptions of alleged restrictions in legal acts, lower level regulations, administrative requirements, policy documents, etc. and they might be particularly related to implicit requirements as highlighted above. User preferences might also be related to a lack of trust or confidence in cross-border data flows. User preferences might of course also be related to other factors, such as preferences related to language.