Deutsche Börse Group
Response

to the working group on cloud switching/ porting data

"Draft Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services"

published for consultation on 11 June 2018

Eschborn, 02 July 2018

Contact: Marija Kozica
Telephone: +49 (0) 69 211 - 17178
Telefax: +49 (0) 69 211 - 13315
Email: marija.kozica@deutsche-boerse.com

A. Introduction

Deutsche Börse Group (DBG) welcomes the opportunity to comment on SWIPO Working Group consultative document 'Draft Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services' published 11 June 2018.

DBG operates in the area of financial markets along the complete chain of trading, clearing, settlement and custody for securities, derivatives and other financial instruments and acts as such as a provider of highly regulated financial market infrastructures.

Deutsche Börse AG, the parent company of DBG, operates the largest German Stock Exchange, including regulated markets for equities, exchange-traded funds, certificates as well as options and is as such one of the largest market operators in Europe. For DBAG and its affiliated companies Clearstream Banking S.A., Luxembourg and Clearstream Banking AG, Frankfurt/Main, acting as (I)CSD, as well as Eurex Clearing AG as a leading European Central Counterparty (CCP) for derivatives and financial instruments, operational reliability, data availability and a high degree of data integrity are of utmost importance.

Due to the business-related importance of state-of-the-art IT-systems as well as the scalability of business, DBG has started early to investigate the potential use of the whole spectrum of cloud solutions, including PaaS, IaaS as well as SaaS, and entered into intensive communication with major cloud service providers, competent authorities, standard setting organizations and peers.

We consider a proper regulatory treatment as well as a corresponding development of self-regulatory codes of conduct by the industry as equally important in order to implement an appropriate, sophisticated and comprehensive framework for the use of cloud solutions across industries. Therefore, we appreciate the working group's intention to facilitate the use of cloud computing infrastructures within the EU by developing a common code of conduct on data portability and switching of cloud services. Nevertheless, we are of the opinion that the current draft version of the code of conduct does not provide the necessary level of detail in order to assist users of cloud computing infrastructures (Cloud Service Customers; CSC) to set up the necessary technical and contractual framework to port data or switch cloud computing infrastructures, particularly in case of unexpected events. Further, we consider the limitation to IaaS as a drawback in effectively facilitating data porting and switching of services.

As we abstain from answering the questions raised within the questionnaire provided, we would like to outline our general (Part B) as well as selected specific comments (Part C) on the draft code of conduct below, whereas we have included our insight and knowledge concerning the current developments on cloud computing solutions respectively.

B. General comments

➢ Definition "Code of Conduct"

Notwithstanding the use of the term "code of conduct" within Article 6 of the 'Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union' (COM(2017)495), we would like to point out, that the term "code of conduct" generally refers to a set of rules, norms, principles, as well as values guiding the behaviour, decisions, procedures and systems of an organization or individual. Following Article 6 ibidem those shall serve as the baseline for developing guidelines on best practice providing assistance to facilitate porting of data and switching of services.

The draft code of conduct at hand contains elements of both, a code of conduct as well as guidance on concrete technical and contractual aspects to be considered. In case intended, we suggest to clearly distinguishing the norms and values cloud vendors as well as CSCs shall adhere to from best practice on porting data and switching services.

In the following, we will use the term "(draft) code of conduct" for the sake of simplicity synonymously to best practice, as the draft code of conduct at hand predominantly contains aspects rather providing operational guidance than outlining norms and values to be considered.

➢ Structure of the draft code of conduct

The structure of the draft code of conduct is being outlined under Chapter 2 and provides information crucial for understanding the scope and intention of the code of conduct as well as its limitations. Among others, Chapter 9 contains information on the governance structure framing the code of conduct.

In order to provide transparent information facilitating the use of cloud infrastructures, we suggest to clearly distinguish the actual content of the draft code of conduct, namely Chapters 6, 7 and 8, from information governing the development, maintenance and update of the code of conduct, mainly the remaining Chapters. Chapters 6-8 would form the actual code of conduct while the remaining Chapters, most particularly Chapter 9, would form by-laws of the organisation governing the code of conduct.

In case the working group's wish is to keep only one document, we argue in favour of rearranging the structure of the draft code of conduct such that governance arrangement underlying the code of conduct are being illustrated at the beginning of the document in order to facilitate reading of the code.

➢ Reference to Article 6 of the "Free Flow of non-personal Data Regulation"

Following Chapter 3.5 of the draft code of conduct, its intention is to follow the call for a self-regulatory code of conduct facilitating the switching of providers pursuant to Article 6 of COM(2017)495.

According to Article 6 of COM(2017)495 developing self-regulatory codes of conduct shall "define guidelines on best practices in facilitating the switching of providers and to ensure that they provide professional users with sufficiently detailed, clear and transparent information before a contract for data storage and processing is concluded". Furthermore, Article 6 ibidem specifies the content to be covered by the self-regulatory code of conduct. Among others, information on processes, technical requirements, timeframes and charges that apply in case of porting data shall be provided, including information on required IT configuration and minimum network bandwidth.

Although providing valuable information on relevant aspects of data portability and contractual specifications, we deem the current scope and level of detail of the draft code of conduct as not sufficient to meet the expectations of Article 6 of COM(2017)495 fully, as it neither provides information on actual business practice (e.g. reference values) for guidance, nor does it cover all aspects mentioned within Article 6 ibidem. We suggest to extend the draft code of conduct following the expectations of Article 6 ibidem and provide values and information on common structures and processes rather as references and not as necessarily self-binding requirements. Providing specific information on the possible operationalization of relevant aspects already covered by the draft code of conduct will help CSCs to address elements of the overarching technical and contractual framework, which is crucial for preparing for porting data and/or switching services.

- Limitation to IaaS

With reference to the variety of different cloud services, the code of conduct shall only apply to IaaS, as data portability considerations do not necessarily apply to all cloud services in a same way (see. Chapter 1.5 of the draft code of conduct). While we consent to the statement that portability considerations might vary depending on the concrete cloud service used, we expect that a large number of requirements facilitating portability of data and switching of services applicable to IaaS can be applied to PaaS and SaaS as well. Hence, we would appreciate the development of a comprehensive code of conduct, which might contain specific requirements for different service types. Moreover, we regard the portability of IaaS due to its characteristics (i.e. CSC controls its data exclusively) compared to the transfer or switching of PaaS or SaaS as far easier to achieve, particularly as the major cloud vendors dispose of standardizes processes and structures to transfer data related to the use of IaaS. Guidance on how to achieve portability in case of use of PaaS or SaaS is being required stronger from our point of view.

- Validation of the Declaration of Adherence

According to Chapter 5.3, the Declaration of Adherence remains valid for three years for a specific version of the Code. Chapter 5.4.1 foresees further that in case of material changes to the cloud vendor's Declaration of Adherence its declaration should be re-assessed and updated promptly, whereas the CSC should be informed about the change within 48 hours according to Chapter 8.4.

In order to increase reliability on the code of conduct, we suggest amending Chapter 5.3. in such way, that it is "generally valid and binding" for three years. The requirement to inform the CSC within a period of 48 hours in case of changes to its Declaration of Adherence might be read as an implicit

permission for the cloud vendor to change its adherence before the period of adherence of three years did expire. A material change in the cloud vendor's adherence to structural and technical elements of the code of conduct affecting portability of data and switching of services should only be possible in form of an addition or supplement within the three years of adherence declared. Consequently, in case of such changes, cloud vendors should be obliged to adhere to the code of conduct they have declared adherence to least, as well as to the one encompassing the changes made (in case applicable). CSCs have to be able to rely on the compliance declared for a set time frame and should not be easily subject to unexpected material changes.

We suggest further that adherence should be declared after two years of the ongoing declaration for the upcoming three years. In case the cloud vendor intends to revoke its Declaration of Adherence, it shall inform its CSCs at least one year in advance to expiration of its Declaration of Adherence.

C. Selected specific comments

- Demonstration of compliance

Chapter 3.1. foresees that the respective cloud vendor, accepting the code of conduct, shall demonstrate its compliance with it. Compliance can be demonstrated either through adoption of standards - whereas it is not further specified, what it to be considered as "standards" - or through certifications such as the ISO/IEC 19941:2017(E), which specifies cloud computing interoperability and portability types as well as further aspects on the relationship and interactions between cloud computing and common terminology. This statement creates the impression that through obtaining the certification of ISO/IEC 19941:2017(E) all aspects of the current version of the draft code of conduct are covered.

While we generally support the approach of obtaining certifications for demonstrating adherence to general industry-wide accepted standards, the exclusive reference to one standard raises the question on overlapping aspects of the code of conduct and ISO/IEC 19941:2017(E). It should be transparent, for which aspects of the draft code of conduct the ISO standard can demonstrate compliance and in which cases the draft code of conduct provides further recommendations. In case ISO/IEC 19941:2017(E) fully covers the aspects recommended by the draft code of conduct, its value added should be questioned and the draft code of conduct should be reviewed critically, where appropriate.

- Contractual specifications

Chapter 7 contains information on the contractual specifications necessary to ensure data portability and switching of services and/ or cloud vendors. Beside exclusively covering contractual specifications on the existing contract between the CSC and the cloud vendor currently used (i.e. phrasing requirements applicable to the cloud vendor containing the data and required to assist in porting data to another cloud vendor or the CSC), we are of the opinion that the code of conduct should also phrase requirements related to the acceptance of data (i.e. requirements applicable to the cloud vendor taking the data or providing the *new* service). This is of particular importance for CSCs without relationships to multiple or mutually substitutable cloud vendors, as we have experienced that negotiating contracts with cloud vendors might require long periods.

- Security of data centres

Although the focus of the draft code of conduct is on portability of data as well as switching of services, we are of the opinion that minimum security standards on physical security of data centres shall be covered by the code of conduct as well. In line with the requirements on the description of location under Chapter 8.2, also the adherence to dedicated standards for data centres such as ISO 27001 or a generic description of key minimum features should be required. We suggest including such requirements under Chapter 8.2. or within a new Chapter 8.5.

- Public Register and non-compliance complaints

According to Chapter 9, a Public Register shall be maintained to provide information on the cloud vendors adhering to the code of conduct as well as contain non-compliance complaints of CSCs against cloud vendors.

As the Public Register will contain relevant information about a cloud vendor and therefore might create reputational risk, further information should be provided on the maintenance of the register as well as the procedures underlying the assessment of non-compliance and publication of a cloud vendors name on either one or both of the "lists" (i.e. list of compliant cloud vendors vs. list of non-compliant cloud vendors). It should be particularly ensured that non-compliant complains will not be published without a prior assessment on their validity. Cloud vendors should obtain the opportunity to comment on the complaint before publication. It might be moreover reasonable to require conflicting parties to enter into conciliation to avoid complaints.

In order to involve both parties appropriately, the standardised procedure for handling non-compliance complaints should include (i) a hearing on the complaint(s) raised, (ii) a submission of statements from both parties as well as (iii) decision to be taken by the Complaints Committee under consideration of the statements obtained from the involved parties.

Another point to be reconsidered with regard to the processing of non-compliant complaints it the assignment of resulting costs. Currently the draft code of conduct foresees, that the party raising the complaint shall bear the costs of the respective complaint according to Chapter 9.2.3. While potential costs might prevent parties to unjustifiably raise complaints, it might also set incentives against complaining, even in case of appropriate complaints.

We therefore suggest implementing an allocation method to absorb the costs resulting from non-compliance complaints at first stage. In case the complaint raised has been identified as justified as the cloud vendor is in breach of the code of conduct, the costs resulting from the processing of a non-compliance complaint should be re-allocated to the cloud vendor in breach. Similarity, costs for complaints obviously unjustifiably raised can (depending on the concrete situation) be fully or partly assigned to the respective complaining party.

- Changes to the code

In case of changes to the code of conduct, the updated version shall be published, whereas the two previous versions shall remain available as well (s. Chapter 10.2). Under consideration of Chapter 5.3, according to which a CSC's Declaration of Adherence shall be valid for three years, we suggest

not to limit the publication of different versions of the code of conduct to maximum three, but instead to keep at least the versions of the last three years, irrespective of their number.

- Executive Board

No more than one person in the Executive Board shall represent one organisation or company according to Chapter 9.1.4. We would like to note that a single entity or group can be a member of an association and hence be represented by it as well as in the same time represent itself separately from the association. We would like to ask the working group to consider such circumstances and adjust the respective requirement.

Moreover, the Executive Board shall have a Chairman and a Vice-Chairman (s. Chapter 9.1.5). We suggest amending this requirement by adding that in case the Executive Board is being chaired by a representative of a cloud vendor, the Vice-Chairman shall be a representative of a CSC and vice versa.

- Complaints Committee

As outlined under Chapter 9.2.1 the Complaints Committee shall be composed of five members, whereas a balanced representation of cloud vendors as well as CSCs shall be ensured. At least one member shall be independent.

As the majority of members usually does not consist of independent representatives, we suggest rephrasing Chapter 9.2.1. such that two representatives shall be adopted by CSCs on the one hand and respectively two representatives by cloud vendors on the other hand. The fifth representative shall be an independent member.

- Remedies against non-compliance

Chapter 9.3 of the draft code of conduct outlines remedies against non-compliance, including enforcement measures, whereas the enforcement measures shall be without prejudice to the customer's rights under applicable EU-law or service agreement. We regard the consideration of applicable EU-law as insufficient and suggest extending the respective requirement to also include national law.

- Term "competent supervisory authority"

The Executive Board reserves the right to seek opinion on changes to the code of conduct of a "competent supervisory authority". As various entities from different industries as well as jurisdiction can be represented within the Executive Board and make use of the code of conduct, we ask you to specify the term "competent supervisory authority" used under Chapter 10.2..

* * *

We are at your disposal to discuss the issues raised and proposals made if deemed useful.

Faithfully,

Jürgen Hillen

Executive Director
Regulatory Compliance

Bastian Bahnemann

Head of Delivery Management