MICROSOFT RESPONSE TO THE EUROPEAN BANKING AUTHORITY'S CONSULTATION ON ITS DRAFT GUIDELINES ON OUTSOURCING ARRANGEMENTS

September 2018

1. Introduction

1.1 The European Banking Authority's (EBA) decision to consult on updating the CEBS guidelines on outsourcing issued in 2006 is a positive step forward given changes that have occurred in the financial services sector in the last 12 years, particularly for institutions and payment institutions (together "**outsourcing institutions**") seeking to transform and innovate with cloud technology in ways which were barely conceived of when the CEBS guidelines were originally drafted.

1.2 As the EBA itself acknowledged when consulting on its 2018 Recommendations on Cloud Outsourcing ("**the Recommendations**") cloud services can offer a number of advantages to financial institutions - including greater ability to innovate and to scale and in terms of offering a infrastructure with enhanced flexibility, business agility, operational efficiency, security and cost effectiveness. Further, cloud can spur greater innovation, and democratise access to financial markets, resulting in increased competition and greater choice of financial services to downstream customers.

1.3 We welcome the EBA's approach to identifying key objectives and core issues. It is essential that the EBA's Guidelines on Outsourcing ("**the Guidelines**") focus on finding practical solutions which can lead a path towards:

- overcoming the outdated nature of the regulatory framework as it applies to cloud services;
- overcoming the lack of EU-wide and broader international harmonisation of regulatory practices;
- recognising that cloud technologies can alleviate many of the challenges that traditional outsourcing arrangements present, by enabling outsourcing institutions to manage risk appropriately. Further, as such services are increasingly becoming standardised, this can streamline risk assurance reviews, providing greater predictability about such cloud frameworks in terms of customer and regulatory oversight, as opposed to custom outsourcing arrangements which are, by design, ad hoc; and
- recognising the importance of maintaining a technology neutral approach towards regulation. Only recommendations that observe the principle of technology neutrality can enable the regulatory framework to remain flexible and responsive to changes brought about by future developments in cloud computing and other innovations as technology is rapidly evolving.

1.4 In this response we therefore address and make recommendations on the following issues:

- Concentration risk;
- Subcontracting;
- Access, information and audit rights; and
- Notifications.

1.5 Accordingly, we call on the EBA to adopt the recommendations set out in this response and provide additional solutions to aspects of the regulatory framework that create unnecessary friction and prevent outsourcing institutions from taking a realistic approach to managing risk.

2. **Concentration risk**

2.1 Paragraph 59 of the draft Guidelines states that (when assessing the risks of an outsourcing arrangement) institutions and payments institutions should balance the expected advantages of the proposed outsourcing arrangement, including any risks which can be managed and mitigated against any potential risks which may arise as a result of the proposed outsourcing arrangement taking into account at least:

"a. concentration risks, including from:

i. outsourcing to a dominant, non-easily substitutable service provider; and

ii. multiple outsourcings to the same or related service providers".

2.2 We consider that, when assessing concentration risk, outsourcing institutions (and competent authorities) should focus on whether a proposed outsourcing materially increases the risk versus the risk inherent in the financial services institution carrying out the activity itself – such that concentration risk should not be considered a factor where the financial soundness and operational resilience of the outsourcing provider is equal to (or better than) the financial soundness and operational resilience of the financial institution itself.

2.3 We also consider that concerns regarding concentration risk should not operate so as to prevent outsourcing institutions from choosing the products and/or services they feel are right for their particular needs. Issues of concentration can be managed principally by ensuring that service providers enable data portability and interoperability with other services, including on-premise applications and services. For example, hybrid portability and compatibility are a reasonable way to address concerns on concentration risk and mitigate issues concerning so-called lock-in. This is particularly true of software-as-a-service (SaaS) arrangements which offer significant benefits in terms of security (since software fixes are applied automatically across the entire network), and feature set (since the customer always benefits from the latest version of the software).

2.4 In the context of Microsoft's cloud architecture, for example, our cloud service arrangements:

- enable data portability and a high level of interoperability with the systems and services of other providers;
- offer flexibility as to the geolocation where data are stored and a high level of transparency as to how the services are operating at all times;
- make use of data mirroring, such that the failure of a single drive (or even the loss of an entire datacentre) does not affect the integrity or accessibility of data that is stored in the cloud;
- support the use of hybrid architectures which enable customers to adopt workloads suitable according to their needs, with an ability to move between traditional legacy on-premises environments and cloud services as desired.

Cloud services therefore can present an increasingly important option for outsourcing institutions in terms of risk mitigation when assessing their technical infrastructure and managing technology expenditure.

3. **Subcontracting**

3.1 Paragraph 59 of the draft Guidelines states that where the outsourcing arrangement includes the possibility that the service provider suboutsources critical or important functions to other service providers, institutions and payment institutions should take into account:

"a. the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country than the service provider;

b. the risk that long and complex chains of sub-outsourcing reduce the ability of institutions or payment institutions to oversee the outsourced critical or important function and the ability of the competent authority to effectively supervise them."

3.2 Whilst we recognise that suboutsourcing has the capacity to increase the risks associated with an outsourcing we consider that the Guidelines should not operate in such a way as to render suboutsourcing impractical, particularly in light of the fact that the EBA acknowledges that suboutsourcing is more dynamic in a cloud context.

3.3 We would therefore urge the EBA to follow Section 4.7 of its Recommendations which expressly acknowledge that notice, rather than prior approval is sufficient:

22. The outsourcing agreement between the outsourcing institution and the cloud service provider should specify any types of activities that are excluded from potential subcontracting and indicate that the cloud service provider retains full responsibility for and oversight of those services that it has subcontracted.

23. The outsourcing agreement should also include an obligation for the cloud service provider to inform the outsourcing institution of any planned significant changes to the subcontractors or the subcontracted services named in the initial agreement that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. The notification period for those changes should be contractually pre-agreed to allow the outsourcing institution to carry out a risk assessment of the effects of the proposed changes before the actual change in the subcontractors or the subcontracted services comes into effect.

24. In case a cloud service provider plans changes to a subcontractor or subcontracted services that would have an adverse effect on the risk assessment of the agreed services, the outsourcing institution should have the right to terminate the contract.

4. **Access, information and audit rights**

4.1 We remain supportive of the EBA's Recommendation that outsourcing institutions should exercise their rights to audit and access in a proportionate and risk-based manner, including through the use of pooled audits or through third-party certifications and third-party or internal audit reports made available by the cloud service provider.

4.2 Specifically, the EBA should continue to follow the principles in the Recommendations, which apply a proportionate and balanced approach to audits:

8. The outsourcing *institution should exercise its rights to audit and access in a risk-based manner. Where an outsourcing institution does not employ its own audit resources, it should consider using at least one of the following tools:*

(a) *Pooled audits organised jointly with other clients of the same cloud service provider, and performed by these clients or by a third party appointed by them, in order to use audit resources more efficiently and to decrease the organisational burden on both the clients and the cloud service provider.*

(b) Third-party certifications and third-party or internal audit reports made available by the cloud service provider, provided that:

i. The outsourcing institution ensures that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and the controls identified as key by the outsourcing institution.

ii. The outsourcing institution thoroughly assesses the content of the certifications or audit reports on an ongoing basis, and in particular ensures that key controls are still covered in future versions of an audit report and verifies that the certification or audit report is not obsolete.

iii. The outsourcing institution is satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, reperformance/verification of the evidence in the underlying audit file).

iv. The certifications are issued and the audits are performed against widely recognised standards and include a test of the operational effectiveness of the key controls in place.

v. The outsourcing institution has the contractual right to request the expansion of scope of the certifications or audit reports to some systems and/or controls that are relevant. The number and frequency of such requests for scope modification should be reasonable, and legitimate from a risk management perspective.

4.3 In our view such wording continues to achieve the EBA's objective of preventing outsourcing institutions from inappropriately relying on use third-party certifications and third-party reports whilst at the same time striking a balance which would enable outsourcing institutions undertaking lower risk outsourcings to benefit from the cost savings associated with use third-party certifications and third-party reports. This contrasts with the proposed language in sub-paragraph 74 of the draft Guidelines which appears to remove an institution's ability to strike such a balance.

4.4 Finally we note that whilst sub-paragraphs 75(a)-(f) of the draft Guidelines appears to reflect sub-paragraphs 8(b)(i)-(v) of the Recommendations, they do so in the context of pooled audits and not (as is the case under the Recommendations as outlined above) in the context of third-party certifications and reports. Whilst we can see the logic of applying those criteria against the conduct of pooled audits we consider that they should apply equally to third-party certifications.

5. **Notifications**

5.1 Unlike in other regulatory contexts, the EBA has not taken the approach of prescribing the form in which outsourcing institutions should communicate with competent authorities on entering into a material outsourcing arrangement.

5.2 Uncertainty as to the amount of information and the process for engaging with competent authorities creates a significant administrative burden for some outsourcing institutions, particularly those that are smaller in size or do not otherwise have a designated supervisory contact. This problem is magnified in the context of an outsourcing that affects services which are provided across multiple jurisdictions. Accordingly, we advocate the view that competent authorities should standardise their approach to requesting information in respect of technology outsourcing and cloud service arrangements such that a financial institution looking to undertake such outsourcings do not have to prepare separate notifications (involving different sets of forms) for each jurisdiction which will be impacted by the outsourcing.

5.3 We would therefore urge the EBA to take the lead in developing a single, standardised form of outsourcing notification in order to minimise the overall cost of compliance with the Guidelines' notification and due diligence requirements and to harmonise the notification process. To aid the EBA in that effort we have produced an example standard notification of outsourcing form (see Appendix I, below) to act as a jumping off point for developing such a notification.

APPENDIX I -
PROPOSED FORM OF OUTSOURCING NOTIFICATION

<*Location*>, <Date>

To <*Name of supervisory office*>,
Attn. <*Full Name*>, <*Function Title*>
<*Department/Division*>
<*Name of regulatory body*>

Re: Notification on implementation of <*Product and/or Service Name* > in <*Organization*>.

Dear <title>,

Further to the decision to <*decision summary*> approved by the <*accountable decision body name*> on <*date of decision*>, <*organization*> is preparing to outsource the performance of certain critical or important functions within <*organization*>.

Info: The purpose of this notification cover letter is to inform the financial or privacy supervisor that appropriate internal due diligence processes have been involved prior to approving the service. There is no need to highlight individual risks & project details. Instead, the letter should explain the internal risk governance processes that have been followed, outline internal responsibility and ownership over the solution and its involved risks.

Recommended sections to highlight in the cover letter (2 to 3 pages):

1. *Context*
    - *Short service description*
    - *Scope & timeline of the project*
    - *Impact on data processing (type of data that is processed in the cloud, in which countries will this data be processed)*
    - *Internal ownership over the solution (IT, Business, group vs. local)*
2. *Benefits & decision*
    - *Key benefit of the solution, why was the decision made (context)?*
3. *Risk management*
    - *Summary of the internal risk assessment process & risk approval (which of the management functions have been involved in the approval, who chairs these decision body members etc.)*

- *Applicable regulations that have been considered (include both financial as well as privacy regulations).*
- *Statement on audit rights & right of access by financial supervisors*
- *Statement on service resilience, business continuity & exit strategy*

4. *Annexes*

    - *Supervisory Notification Sheet (template)*

Supervisory Notification Sheet Part 1 - Overview

SUPERVISOR QUESTIONS	CLARIFICATION (ANSWER FIELD)
Unique Identifier or Reference	<Unique identifier linked to the outsourcing arrangement>
Description of outsourced activity (Process/Function/Activity)	<Description of the outsourced activity & sub-activity within the FSI (e.g. Customer Relationship Management / Customer Acquisition, or Risk Management / Liquidity Controlling). Include a clear self-explanatory description, without use of jargon or abbreviations.>
Assessment of the criticality or importance	<Brief description of the basis upon which the institution or payment institution considers the outsourced activity is critical or important>
Name of the Service Provider (SP)	<Name>
Country where the SP is registered	<Country>
Region where the service will be provided (incl. countries of data storage)	<In which countries will the services be provided? If applicable, in which countries will data at rest be stored?>
Contractual service start date	<Date>
Next contractual renewal date (or service end date)	<Renewal/Service End Date>
Applicable laws governing the contract	<The law governing the contract, as defined in the contract.>
Parties receiving service under the outsourcing arrangements	<These are the entities that are using the service. This may be the name of the financial institution at group level, or a set of specific subsidiaries from the institution.>
Approval date for the outsourcing + decision body	<Highest decision body within the accountable business line.>
Relationship Manager within the institution or payment institution	<Individual responsible for managing the relationship/contract with the SP>
Relationship Manager within the SP	<Key contact person within SP overseeing the SP relationship (e.g. account manager)>
Data Privacy Officer (DPO) within the Bank	<Relevant only when processing personal data of EU citizens context of GDPR, otherwise use N/A to indicate that no personal data is processed in the system. >
Data Privacy Officer (DPO) contact within the CSP	<Relevant only when processing personal data of EU citizens context of GDPR, otherwise use N/A to indicate that no personal data is processed in the system.>

Name(s) or list of subcontractors + countries where these are registered	<Relevant only where subcontractors will be used>
Date of the latest materiality assessment for the service?	<Date>
Does the service involve time-critical functions (Y/N)?	<Yes><No>
Assessment of the outsourcing providers substitutability	
Identification of alternate service provider(s)	
Date of the latest risk assessment	<Date>
For outsourcing in respect of Cloud Service Providers (CSPs) only:	
Cloud deployment model (public/hybrid/private)	<Private Cloud><Public Cloud><Hybrid Cloud>
Licensed Products in scope + number of users	<Reference to the specific cloud services that are consumed, as well as the targeted use of any licenses>

Supervisory Notification Sheet Part 2 – Overview Compliance with Outsourcing & Privacy Guidelines

KEY REQUIREMENT	HOW MET
Written Agreement: The outsourcer should ensure that there is a written agreement in place which sets out the responsibilities of both parties.	
Right of Access; Right to Audit: a) The contract must allow the outsourcing institution's compliance and internal audit departments complete access to its data and its external auditors full rights of inspection of that data; and b) The contract should allow direct access by the outsourcer's supervisory authority to the outsourcer's relevant data and premises.	
Termination Rights: The contract shall allow the outsourcer to cancel the contract on notice or extraordinary notice of cancellation if required by the regulator.	
Exit Provisions: The contract should include termination and exit management provisions which allow the outsourced activities to be transferred to another service provider or to be reincorporated into the outsourcer.	
Use of Sub-Contractors	

The contract should take account of the risks associated with chain outsourcing.	
Data Security Appropriate security measures such as access controls, cryptographic protections, cybersecurity defences & monitoring must be established.	
Notification of Security Breaches Contractual commitments to report security breaches within 72 hours.	
GDPR Compliance Processing of personal information of European citizens must occur in compliance with the EU General Data Protection Regulation (GDPR).	