



**MICROSOFT RESPONSE TO THE EUROPEAN SECURITIES AND MARKETS AUTHORITY  
CONSULTATION PAPER – DRAFT GUIDELINES ON OUTSOURCING TO CLOUD SERVICE PROVIDERS**

**1 September 2020**

1. Microsoft welcomes the European Securities and Markets Authority (“ESMA”) Consultation Paper on Outsourcing to Cloud Services Providers (referenced as “Consultation Paper” in this response). We believe that this Consultation Paper is the logical next step to provide clarity for regulated institutions subject to oversight by ESMA, as other regulatory authorities in Europe have similarly issued guidance on outsourcing, including the European Banking Authority (“EBA”), European Insurance and Occupational Pensions Authority (“EIOPA”) and, still under consideration, the UK Prudential Regulation Authority (“PRA”). We view these regulatory guidance papers as a positive step towards driving harmonization and convergence, which is important for financial institutions and for technology providers alike.
2. As the ESMA Consultation Paper on the whole, is fairly consistent with guidance issued by the EBA and EIOPA, we narrow our comments principally to areas where either we see some potential divergence from guidance issued, or where some drafting remains ambiguous, and further clarity would be helpful. Similarly, we think it is appropriate to compare the UK PRA’s Consultation Paper on Outsourcing and third party risk management, though not closed, is equally designed to address the same issues and drive towards harmonization on regulatory guidance with authorities on the Continent.
3. The ESMA Consultation Paper provides a comprehensive framework as the regulator guidance and consultation papers referenced above, but it omits two key elements we think should be built-in to this guidance to provide for flexibility and adaptability to new innovations, given the dynamic and disruptive change that is ongoing.
  - First, we think that, as a threshold matter, it should be clear the guidance is principles based, focusing on outcomes in managing risk, not prescriptive measures how to address such risk. This is needed for a few reasons, including (i) managing risk is not a one-size-fits-all solution for all institutions, (ii) innovative technologies may provide for different approaches, and institutions should have flexibility in choice of which approaches they implement, and (iii) the pace of innovation and dynamic change will require ongoing agility to address new and better ways of managing risk going forward.
  - Second, the EBA and UK PRA Consultation Paper on Outsourcing and third party risk management apply a tech-neutral approach to outsourcing – one we think is appropriate to give clarity to institutions that managing risk cuts across all forms of outsourcing – no special or different rules are required for cloud computing. In our experience, customers tend to place emphasis on a different set of requirements for cloud outsourcing, including seeking to impose controls not even addressed in their own current environments. A technology neutral approach focuses on underlying controls in managing risk equally, without treating cloud computing better or worse relative to existing legacy environments. This consistency in approach by regulators, and financial institutions, is important to assess risk appropriately.

Thus, we think it is important to drive harmonization, and clarity, that the guidance be clear it is principles based, and technology neutral in approach.

4. Data Privacy and Data Localization. Paragraph 9 of the Consultation Paper infers that data location in Europe is required. It states:

These risks relate to the governing law of the firms' contract with the cloud service provider, as well as the data location requirements. In particular, EU personal data location requirements require close consideration.

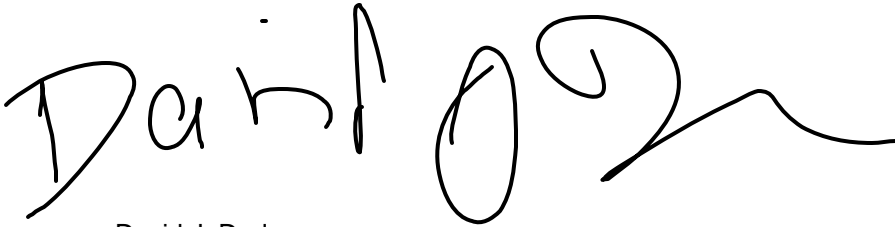
We agree that legal risks in understanding where data located is required, as well as transparency about where data is stored is important for assessing legal risk, but any inference that data must be stored in Europe is misplaced. To provide for consistency in approach with other regulatory guidance issued, including permissibility of data being stored outside of Europe, we suggest this be modified, in line with EBA and EU guidelines, that the agreement set out "the location(s) (i.e., regions or countries) where the critical or important function will be provided and/or where the relevant data will be kept and process, including the possible storage location."

5. Concentration Risk. Two elements concerning concentration risk we think should be further clarified:
  - Paragraph 33 (v) states for critical and important functions that a firm assess "the portability of the data of the firm, namely the capacity to easily transfer the firm's data from one CSP to another." As a point of clarification, we think this should be clear what is needed is for the firm to have appropriate exit strategies in place, including documentation of such plans, testing, and overall project management and roles in implementation. This would be consistent with what is referenced in the EBA guidance (see Paragraphs 106-108).
  - Paragraph 33 (vii) states that firms should assess "possible concentration within the firm (including, where applicable, at the level of its group,) caused by multiple cloud outsourcing arrangements with the same CSP as well as possible concentration within the sector, caused by multiple firms making use of the same CSP or a small group of CSPs." Firms have no capability to assess systemic risk at a macro level. That is within the function of regulators, and is firmly addressed in the EBA Guidelines(See Paragraph 45 – "Competent authorities need to identify the concentrations of outsourcing arrangements at service providers.")
6. Exit Strategies. Paragraph 44(c) requires that, for critical or important functions, the financial institution impose the following obligation on the CSP: "ensure that the cloud outsourcing written agreement includes an obligation for the CSP to orderly transfer the outsourced function and all the related data from the CSP and any sub-outsourcer to another CSP indicated by the firm or directly to the firm in case the firm activates the exit strategy." As referenced above, this obligation should be on the financial institution itself, and such obligations clearly remain with the financial institution in the EBA guidance as referenced above. Instead, we suggest that it is appropriate to require that the CSP "enable" the customer to terminate and exit the agreement, to fulfil its regulatory requirements such as a material impairment in the service. We suggest the following language for your consideration: "ensure that the cloud outsourcing arrangements written agreement allows for the transfer of the outsourced function and all the related data from the CSP and any sub-outsourcer to another CSP defining support obligations towards the CSP in case the firm activates the exit strategy."
7. Sub-Outsourcing. As a matter of clarification, we think the provisions concerning sub-outsourcing of critical or important functions should be, in total, read together. In essence, this means that while an institution should be informed of a new sub-outsourcer providing critical or important functions, and the right to object, its ultimate recourse is to terminate an agreement if such resolution cannot be mutually agreed to between the parties (Paragraph 55 f). It is not practical for any one institution

“hold up” use of a sub-outsourcer providing critical or important functions, particularly given when other institutions do not object to the outsourcer. We read the spirit of these provisions to mean this is the underlying intent but further clarification may be helpful in this regard.

We would be pleased to discuss further with ESMA concerning this consultation at your convenience.

Sincerely,

A handwritten signature in black ink, appearing to read "David J. Dadoun". The signature is fluid and cursive, with a large, stylized "D" at the beginning and a long, sweeping tail at the end.

David J. Dadoun

Managing Direct, Global Regulatory Compliance, Worldwide Financial Services Industry Team

ddadoun@microsoft.com

Mobile: +1-206-293-0794