ECSDA Response to the ESMA Consultation Paper on Outsourcing to Cloud Services Providers

ECSDA Executive Summary

The European Central Securities Depositories Association (ECSDA) welcomes the consultation paper on Draft Guidelines on Outsourcing to Cloud Service Providers.

We believe that some elements in this consultation would benefit from alignment with the EBA Outsourcing Guidelines, while others would benefit from clarification, given the specific context of CSDs as FMI. ECSDA considers that a single set of guidelines which would apply to all outsourcing relationships and thus integrate both cloud and non-cloud outsourcing would be the ideal methodology to follow if it is taken into account that only some CSDs are subject to the EBA Guidelines. Careful consideration needs to be given to the interaction between the European Authorities guidelines on outsourcing to CSPs and eventual related legislative developments. Those legislative efforts of enhancing coherence would gather our support, as they would alleviate the industry from some significant concerns related to contract management.

Main comments

1. Further alignment is needed on definitions and exemptions with EBA guidelines and CSDR

Although not all CSDs are subject to the EBA Guidelines, only those CSDs having a banking license, we believe the definitions used in EBA guidelines should be clarified and further aligned across financial regulation and all EU authorities. While the purpose of each of the guidelines issued by the different authorities is the same (i.e. protect the businesses and the financial markets), the unalignment or different interpretation of definitions and concepts create confusion, prevent consistent approach throughout the industry and lead to reconciliation issues between authorities.

We propose that the ESMA guidelines refer to an existing definition of outsourcing, or include a new one, ensuring consistent scope between the ESMA and EBA guidelines.

A **single and concise definition of a critical or important function** should also be included. In relation to CSDs, the existing definition of 'critical or important function' is unclear.

In addition, it should be acknowledged that **not all cloud arrangements should automatically be considered as outsourcing**, which is clearly acknowledged by EBA guidelines.

In the same vein, as EBA does not consider clearing and settlement activities performed by FMIs as outsourcing, **we would appreciate ESMA to mention explicitly that FMIs, as they are already subject to the specific requirements,** are not expected to be bound by the application of the guidelines by their respective participants.

CSDs and the entities covered by the CPMI-IOSCO Principles for FMIs are subject to very high standards and controls in terms of security, confidentiality, availability, and resilience. In the EU legislative framework, these principles have been transposed into EU legislation (EMIR and CSDR). EU CSDs are hence subject to a specific harmonized regulatory framework for CSD services such as safekeeping, settlement, asset servicing and collateral management.

In our view, this regulatory framework warrants our counterparties with the necessary protection and comfort and, hence, does not justify the need to grant access or audit rights for example. Such rights could create operational and security risks for CSDs and thus, could ultimately impact financial stability.

2. The guidelines should take a principle-based approach

We support the policy intention of the CSP outsourcing guidelines. Nevertheless, we believe that the requirements being imposed may exceed the industry's capacity to ensure compliance. ESMA may wish to introduce off-setting measures given the amount of control that institutions are able to exercise over some of the CSPs on a stand-alone basis.

Alternatively, we would advise for the guidelines to become more principle-based, notably on some of the contractual provisions (e.g. how to include certain wording in the agreements). This would support a smoother transition to new and cloud-based technologies.

We note the below examples where a principle-based approach would be preferable:

a. Contractual provisions in the CSP arrangement (see ECSDA response to guideline 3)
b. Management of sectorial concentration risk (see ECSDA response to guideline 2)
c. Audit requirements (see ECSDA response to guideline 6)

3. Intra-group outsourcing should be framed more explicitly

CSDR has specific provisions on outsourcing for CSDs which are largely aligned with the provisions of the EBA Outsourcing Guidelines. Similarly, any guidelines on outsourcing should explicitly cater for the central performance of certain functions by the parent company or other companies for the benefit of the group. For example, a CSD should be able to use a CSP outsourcing governance framework developed from a parent group for all subsidiaries.

In addition, we believe that the requirements on intra-group outsourcing could be proportionate in comparison with those imposed on external third-party providers. Intragroup outsourcing could be subject to lower obligations than extra-group third-party outsourcing agreements or the obligations could be looked at in a more pragmatic way. Indeed, an intragroup structure implies that a common interest and regulatory oversight from the parent's regulator or from the

service provider regulator already exists. The guidelines should recognise the degree of integration reached within groups of regulated entities regarding documentation, due diligence, concentration risk and exit strategy.

Complementary comments on ESMA Guidelines

Guideline 1.
Governance, oversight and documentation

Q1: Do you agree with the suggested approach regarding a firm's governance and oversight in relation to its cloud outsourcing arrangements? Please explain.

ECSDA response

Complementary information to our "Main comments" section

Governance and oversight of cloud arrangements should not be separate or additional process but it should be a part of the firm's vendor management process, which includes the risk-based approach, monitoring of vendor performance, SLA etc.

The purpose of register of information on all cloud outsourced arrangements and practical use of it is not clear. Who and in which cases should use the register? Some data (e.g. annual cost) could be considered as excessive. In our view, the summary of the reasons when the outsourced function is or is not critical is defined in other systems of functions registers and should not be duplicated. However, other valuable information such as the type of cloud service (IaaS, Paas, Saas etc) might be missing.

Q2: Do you agree with the suggested documentation requirements? Please explain.

ECSDA Response

Complementary information to our "Main comments" section

Art. 29 of the Draft Guidelines lists the information to be included in a register. We believe some flexibility with respect to the format would be preferable. Having to set up new records, templates and registers for information that is already properly recorded would, in our view, be disproportionate. It would be preferable not to implement a single template or format, but, for the regulated entities, to confirm that the requirement can be met with different formats.

With respect to CSDs, the CSDR framework requires that the outsourcing by CSDs of their services or activities to a third party must also comply with specific requirements. Notwithstanding the abovementioned, we believe that the commercial aspect of the

outsourcing agreement, i.e. the costs as described under Art. 29 (m) do not need to be included, as they would not impact the regulatory goal of this register.

It is not clear how Art. 30 relates to the requirement in Art. 28 and 29 to only include further detailed information on outsourcing with respect to critical or important functions. We would suggest leaving out any requirement to include non-critical functions. Otherwise, it would lead to diverging interpretations and unclarity as to what further information to include, ultimately leading to a disproportionate workload. The register should be limited to critical and important functions only.

Guideline 2.
Pre-outsourcing analysis and due diligence

Q3: Do you agree with the suggested approach regarding the pre-outsourcing analysis and due diligence to be undertaken by a firm on its CSP? Please explain.

ECSDA response

Complementary information to our "Main comments" section

We generally agree with the suggested approach. Pre-outsourcing and due diligence of cloud arrangement was to be in the same process as other vendor assessment process before outsourcing of any function.

Management of sectorial concentration risk: The requirement for financial institutions to maintain a register creates transparency on concentration risk toward CSPs. While we acknowledge the value of monitoring possible concentrations within firms, a firm would not be capable of monitoring possible concentrations towards CSPs within its sector.

Hence, we ask ESMA to remove the sectorial risk monitoring requirement. We believe that the publication of the register to NCAs will allow public authorities to monitor such risk. In addition, for the benefit of harmonisation, we also note that the requirements on the content and/or format of the register should be the same for all Competent Authorities.

Guideline 3.
Contractual requirements

Q4: Do you agree with the proposed contractual requirements? Please explain.

ECSDA response

Complementary information to our "Main comments" section

Contractual provisions in the CSP arrangement: A supervisory framework for ICT third party providers to financial institutions is an important step towards managing the risk of vendor lock-in and fostering innovation. It will also contribute to ensure the right balance between imposing

requirements on the users of CSP services versus expecting compliance from CSPs themselves (especially those that become of systemic importance).
Notably, when it comes to provisions on the transferability of services and exit plans, we believe that the remit of the draft guidelines goes beyond what financial institutions can reasonably control. For example, the obligation to request a mandatory insurance coverage from CSPs. The reason for it is not clear for us. In particular, whether it is due to the activity of the firm, we would appreciate clarifications on this point. In the best scenarios, we are able to obtain a certificate of a CSPs current insurance coverage. It remains the responsibility of the user to accept the service provision terms of the CSP, hence CSPs will in general not be inclined to adapt their terms to individual clients. Offering standardized services is part of the business model of many CSPs. Therefore, we would much appreciate your considerations with regard to the situation.

Guideline 4.
Information security

Q5: Do you agree with the suggested approach regarding information security? Please explain.

ECSDA response

Complementary information to our "Main comments" section

We consider that the controls identified in the consultation concerning information security requirements are generally reasonable. In addition, IT security has clearly to be distinguished from data protection, as these have different implications. We would also much appreciate further coherence of the proposals with the existing terminology.

Guideline 5.
Exit strategies

Q6: Do you agree with the suggested approach regarding exit strategies? Please explain.

ECSDA response

Complementary information to our "Main comments" section

Regarding the exit strategies and their activation, the idea of ensuring the obligation for the CSP to orderly transfer the data to another CSP in such a case is welcomed. On the other hand, the requirement to identify and develop in advance transition plans could be a burden, in particular to small firms.

In addition, we have several other comments:

- For Art. 44a and 45e, as exit plans do often mean significant efforts (i.e. for migrating application and data), testing may not be possible in many cases. This could be a burden for firms to pick-up the new technology, as e.g. code would need to be rewritten and retested during operations, which would result in very high efforts.

- For Art. 44c, it might not be feasible in practice. CSPs might be willing to offer a kind of "transfer system".
- For Art. 44d, we would appreciate further regulatory advice on how a firm could guarantee that its data is removed or deleted by the CSP. Currently, the solution that we see is that the CSP and the outsourcing company would have a contractual agreement to delete the data. Similar provisions are already used in the Art. 28 (3) g) of GDPR.

Guideline 6.
Access and audit rights

Q7: Do you agree with the suggested approach regarding access and audit rights? Please explain.

ECSDA Response

Complementary information to our "Main comments" section

Audit requirements: We appreciate the possibility of certifications or pooled audits in order to oversee the CSP. We note, however, the reference to pooled audits which are to be performed jointly with other clients of the same CSP or by a third-party auditor appointed by multiple clients of the same CSP. We wish to learn how institutions need to be aware of and arrange such with other clients of that CSP.

We also seek clarification on the interaction between Art.50 and Art.52 (Guideline 6). It is unclear whether institutions, in any case, need to perform a 'complete audit', even when they meet the conditions of Art.50 and thus regardless of pooled audits or certifications.

For Art. 51, we are wondering how a firm could effectively extend the scope of any third-party certification scope. Particularly for Art. 51f, today, some CSPs grant the right to give an expansion. However, as of now, contractual arrangements are varying. From a customer perspective, it would be helpful if this would be a legal requirement to grant the request.

Guideline 7.
Sub-outsourcing

Q8: Do you agree with the suggested approach regarding sub-outsourcing? Please explain.

ECSDA response

Complementary information to our "Main comments" section

We agree with this point and would propose the following process: there should be a notification about the fact of CSP´s using sub-outsourcing to allow the customer to organise an internal risk assessment, including the right to object to the sub-outsourcing and the right to terminate if a CSP would ignore the objection.

It is not clear to us how to implement the requirement in Art. 56 that firm should ensure that the CSP appropriately oversees the sub-outsourcer.

Guideline 8.
Written notification to competent authorities

Q9: Do you agree with the suggested notification requirements to competent authorities? Please explain.

Overseeing by competent authorities of outsourcing to cloud providers should not stand out of outsourcing of other critical or important functions.

Guideline 9.
Supervision of cloud outsourcing arrangements

Q10: Do you agree with the suggested approach regarding the supervision of cloud outsourcing arrangements by competent authorities? Please explain.

ECSDA Response
Complementary information to our "Main comments" section

We agree with the suggested approach but note some further guidance with respect to cross-border groups operating multiple regulated entities might be required. Of course, NCAs should be able to execute effective oversight. With respect to cloud outsourcing, however, this is often done at a group level. We would wish to avoid duplicative efforts by NCAs when the guidelines underpinning this are ESMA-based. NCAs involved in group oversight could coordinate supervisory efforts with the aim to avoid multiple audits in a relatively brief period. Overseeing by competent authorities of outsourcing to cloud providers should not stand out of outsourcing of other critical or important functions.

Q11: Do you have any further comment or suggestion on the draft guidelines? Please explain.

ECSDA response

Complementary information to our "Main comments" section

The Guideline puts big overhead to CSD's when it comes to outsourcing of critical or important functions to the cloud. In many cases, the guidelines are excessive or duplicative from the risk-based governance approach. We fear that it may stop or slow down the progress in the use of technologies for supporting of CSD's functions.

Q12: What level of resources (financial and other) would be required to implement and comply with the guidelines and for which related cost (please distinguish between one off and ongoing

costs)? When responding to this question, please provide information on the size, internal set-up and the nature, scale and complexity of the activities of your organisation, where relevant.

ECSDA response

ECSDA and its members could not be estimating the resources at this point.

About ECSDA

ECSDA represents 41 national and international central securities depositories (CSDs) across 36 European countries. The association provides a forum for European CSDs to exchange views and take forward projects of mutual interest. It aims to promote a constructive dialogue between the CSD community, European public authorities and other stakeholders aiming at contributing to an efficient and risk-averse infrastructure for European financial markets.