Electronic Money Association
68 Square Marie-Louise
Brussels 1000
Belgium
www.e-ma.org

José -Manuel Campa
Tour Europlaza
20 avenue André Prothin,
92400 Courbevoie
France

9 October 2025

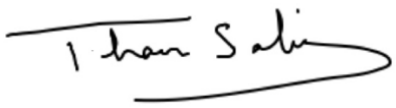
Dear Mr Campa,

Re: EBA Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our head office is in Brussels, and we have branches in Ireland, the Netherlands, Luxembourg, Lithuania, and Malta. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, mobile payment instruments and crypto-asset services. Most of our members operate across the EU, most frequently on a cross-border basis. A list of current EMA members can be found here.

Overall our members welcome the updated Guidelines, as they will provide clarity for regulators and the market. Please find attached our response to the questions posed by the EBA in the Consultation Paper Referenced above.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

List of Questions for Consultation

Q1: Are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?

A. The EMA supports the scope of these draft Guidelines and the focus on non-ICT related services (per Par. 7 in *Subject matter, Scope and definitions*) to avoid confusion and inconsistencies with the third-party risk management requirements for TPSPs that deliver ICT services in the DORA regulation. Ideally, in-scope entities should be able to deploy a single, integrated risk management framework to track third-party risks for all TPSPs that deliver (ICT and non-ICT) functions.

We invite the EBA to provide additional clarity on whether risks associated with the use of TPSPs that provide any of the functions listed in Annex I using ICT channels should be managed under these Guidelines or under DORA? For example, a number of Administrative Services or Customer Services that are listed in Annex I[1] are typically provided over ICT channels and can give rise to ICT-related risks.

We support the proposed two-year transition period afforded to in-scope entities to ensure their third-party arrangements comply with the requirements in these Guidelines. This approach is consistent with the approach adopted by the ESAs to allow in-scope entities to revise their enterprise risk management frameworks to align with DORA requirements.

Q2: Is Title II appropriate and sufficiently clear?

A. Per our comment above, we invite the EBA to provide further guidance on which third-party risk management requirements[2] should apply to non-ICT functions provided by third-party providers over ICT channels. We note that DORA introduces additional detailed requirements on the identification of such third-party providers in the DORA Register of Information that extend beyond these Guidelines. We perceive that the indirect guidance provided on this topic in Par. 31 (p.27) is open to varying interpretations by PSPs and by national competent authorities (NCAs) and can give rise to inconsistent compliance expectations.

[1] Document Management and Archiving; customer contact services & call centre
[2] DORA or these Guidelines

We support the consistent definition of Critical or Important functions (CIFs) in these Guidelines and in DORA which will allow PSPs to design a common methodology to identify these functions and to map the role of TPSPs in their delivery.

We invite the EBA to remove the last bullet point in *Clause 37b*[3] which reads inconsistent with the other risk factors listed in this Clause.

Q3: Are Sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?

A. We invite the EBA to abide by the principle of Proportionality listed under Title I of the Guidelines and to streamline the information that in-scope entities are required to record in the revised Register of Information on Third-Party arrangements listed in *Paragraphs 63 & 64*. Specifically:

- Remove the reference to a *subcontractor* in *Par. 63d*. The Register is intended to record details of TPSPs that have a direct relationship with in-scope entities.
- Remove the requirement to identify the ultimate parent company of a TPSP and provide an identifier for that entity that appears in *Par. 63g*. Note that in-scope entities typically have a documented service delivery agreement with the TPSP and not with their ultimate parent company. Additionally, many ultimate parent companies that are based outside the EU/EEA do not have access to a LEI or to a EUID.
- Remove the requirement to record the country where the function is to be performed (*Par.63h*); this requirement should be limited to TPSPs that provide Critical or Important Functions (CIFs) listed in *Par.64*.
- Remove the requirement to list & identify alternative TPSPs in the Register (*Par.64g*)

Q4: Is Title IV of the Guidelines appropriate and sufficiently clear?

[3] vi. where applicable, recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation

A. We invite the EBA to provide more guidance on the scope and methodologies that apply to the risk event scenario analysis that in-scope entities are advised to carry out as part of the risk assessment of third-party arrangements (in *Par. 75*) . Our perception is that such analysis should in any case be limited to TPSPs that support the delivery of CIFs.

We propose that the scope of information that is recorded in written third-party agreements is rationalized to align with the principle of Proportionality listed in Title I. Specifically:

- Remove the reference to identify the location where the function will be provided in *Par. 85b*. We propose that this information is only recorded for TPSPs that support CIFs as listed in *Par. 86*.
- Remove the reference to the obligation of TPSPs to fully cooperate with competent authorities in *Par. 85k*. We propose that this obligation applies only to third-party agreements TPSPs that support CIFs as listed *in Par. 86*. Note that many TPSPs that support non-CIFs deliver their services to in-scope entities through generic Software as a Service (SaaS) agreements and are sometimes based outside the EU/EEA. The willingness of such entities to amend their existing agreements to abide by EU requirements is limited as demonstrated by the ongoing difficulties that PSPs face to attain compliance with similar DORA requirements for TPSPs that deliver ICT services.

We invite the EBA to clarify the requirement detailed in *par. 89* that references recording in the Register if a CIF is subcontracted. The Register of Third-Party Arrangements (as detailed in *Par. 63 & 64*) records the details of specific TPSPs that deliver operational functions rather than operational functions that may be provided by TPSPs.

We advise that the requirement for TPSP subcontractors to provide to the financial entity (and to the relevant NCAs) the same type of access/inspection/audit rights as the TPSP is removed from *Par. 90h*. A number of subcontractors offer generic support services to a range of industries and are sometimes based outside the EEA/EU. The path of the financial services industry to attaining DORA compliance has demonstrated that it is quite difficult to convince such subcontractors to revise their standard service delivery agreements to TPSPs to afford such access. We suggest

that TPSPs are afforded more flexibility in ensuring that their subcontractors can provide to them the appropriate data/access rights to allow them to meet the audit/access requirements in the third-party agreements they establish with in-scope entities.

Question 5: Is Annex I, provided as a list of non-exhaustive examples, appropriate and sufficiently clear?

A. As stated in our Response to Question 1, we perceive that many of the functions listed in *Annex I* have a significant ICT component (e.g. *Document management & Archiving, Customer contact services & call center, Regulatory and Supervisory reporting, Payment services - authentication and authorization*). As such, we would expect that the risks associated with the delivery of these functions by TPSPs to in-scope entities are already managed under the relevant DORA risk management frameworks of financial service providers. We invite the EBA to provide further guidance on the management of risks associated with the delivery of such functions to avoid confusion, duplication of effort and inconsistent recording of third-party arrangements across the two frameworks (DORA and these Guidelines) and across EU jurisdictions.