Bundesverband der Wertpapierfirmen e.V.
Federal Association of Investment Firms

Unterlindau 29
D-60323 Frankfurt am Main
Germany
Tel.: +49 69 92 10 16 91
mail@wertpapierfirmen.org
www.wertpapierfirmen.org

Frankfurt am Main, 08.10.2025

bwf comments on the Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk

EBA/CP/2025/12, 8 July 2025

Introductory remarks

The Bundesverband der Wertpapierfirmen (bwf) is representing investment firms and credit institutions throughout Germany whose core activity, or at least a very significant part of their business, lies in the provision of investment services according to MiFID. From a prudential perspective, some members are CRR credit institutions, while most of them are midsized and smaller investment firms (which are still usually categorized as "Class 2" firms according to IFD/IFR resulting from numerous – in our view inappropriate – "zero" thresholds). In this capacity, bwf expressly welcomes the possibility to comment the Consultation Paper (CP) on EBA Draft Guidelines on the sound management of third-party risk.

While we acknowledge that sound and transparent provisions for risk management are important for the stability and resilience of the EU financial system, such rules need to be proportionate with respect to the size, complexity and risk exposure of different financial entities in order to avoid undue administrative burden which can easily result in severe competitive disadvantages for markets within the EU compared to their third country peers, in particular in the UK, the US and Asia.

Currently, the need for "Simplification" of EU financial market regulation (following the program of the new Commission) is the leading topic in almost every conference and policy event in Brussels and throughout the Union. Against this background EBA's proposal, which goes far beyond the existing previous EBA 2019 guidelines on outsourcing arrangements (with a further limited scope on critical and important functions and worthwhile to mention that the guidelines are only applicable to firms which fell under the CRR) by including any "third-party arrangements" (covering principally any contractual relationship with third party service providers – frankly speaking – seems to be completely out of time. In other words, based on a broad feedback by our members and

other trade associations and stakeholders, bwf seems to be not alone in its conclusion that the proposal by EBA – taking into account the insufficient competitiveness of the EU's financial market on a global scale – seems to be completely "out of time" and not only clearly sends the wrong signal at the wrong time but is also clearly overstepping EBA's legal mandate and contradicts the Commissions agenda on simplification and strengthening the competitiveness of the EU.

This said, we would like to answer the questions raised by the CP as follows:

Question 1: Are subject matter, scope of application, definitions and transitional arrangements appropriate and sufficiently clear?

The first question should not be whether the proposed, extremely detailed and far-reaching proposed provisions are "appropriateness and sufficiently clear" but whether EBA has a mandate to impose a substantially extended regime of third-party services monitoring and control (which seems to be de facto duplicating the "DORA-approach" to basically non-DORA-related third-party services and the clear answer is "no"!).

EBA is not a legislator but a supervisor whose authority to further specify existing legislation e.g. by issuing guidelines is bound by a clear mandate and under no circumstances, EBA must exceed its mandate or circumvent legislative decisions which are limited to the Commission, the Parliament and the Council. In fact, we cannot identify any authorization within MiFID II, CRD or IFD which would justify such a far-reaching extension and modification of the existing regime which is limited on outsourcing arrangements of a certain.

Furthermore, the claim of a proportional approach is not convincing at all. De facto, the proposed regime – aside from the missing legal mandate – is based in practice to a large extend on a de facto "one size fits it all" approach, no matter whether we are talking about a systemically important financial entity, a non-systemically-important credit-institution, which is still financed by deposits (which they inevitably put at risk by their business activities) and by investment firms of different size and complexity which usually are funded completely by shareholders' capital and which very often do not even have access to client's assets or money (let alone that they are not systematically important). In particular for "Class 2" investment firms we do not see any convincing rationale to report a significant part of their third-party contractual arrangements as a result of "guidelines" imposed by EBA. This would clearly contradict the principle of proportionality as stipulated by Article 5(4) of the EU-Treaty in conjunction with the long-standing case law of the EU-Court of Justice. From a risk-based perspective, from our point of view (while general concerns regarding the missing mandate remain), only "class 2" firms with direct access to clients' funds or assets could "potentially" be included into the proposed regime. However, it must be remembered that many "real economy" companies often represent a significant credit risk to their (retail) clients, e.g. in form of a down payment for a new car or a residential property without similar obligations.

Furthermore, the additional register planned (and no matter which detailed organizational structure to be chosen) will very likely result (and this would apply add least to the vast majority of "financial entities", no matter whether they are IFD-investment firms or CRR-credit institutions in another completely excessive overly bureaucratic and very expensive (from the industry as well as from a public infrastructural perspective) "data crematory" of little or no regulatory benefit. In fact, EBA's cost impact analysis is not convincing at all and it remains completely unclear how such a huge data-set shall be meaningfully monitored and assessed on an ongoing basis - let alone the problem of enforcing timely and accurate contributions to this additional register. In other words, there is a reason why the scope of DORA was limited in a way which – while already very challenging – might still be manageable.

We would also like to remind EBA that under article 26(4) IFD, EBA is strictly required to involve ESMA in the course of drafting governance requirements under article 26(1) IFD. We are not aware and there is no indication given in the CP whether such a coordination has taken place. Let alone that ESMA just recently (12 June 2025) has published ESMA publishes principles for third-party risk supervision. Even though this paper was addressed at NCAs, it indicates a discrepancy which must raise our concern.

Aside from this, the definitions within the CP seem to be sufficiently clear, even when they are not always proportionate and clearness in wording cannot conceal the lack of a legal mandate.

Question 2: Is Title II appropriate and sufficiently clear?

Due to the lack of legal mandate discussed in question one, it is principally dispensable to address questions two to five in terms of content. Therefore, if we still make selected comments on single topics, we would like to emphasise upfront that this might not be misinterpreted as a relativisation of our fundamental critique of the scope and design of the overall concept as expressed in our answer to question 1.

To begin with, we find it very difficult to establish and meaningfully calibrate a categorization of "contracts that support critical and important functions" on a company wide basis, even for relatively small firms. This is a completely different task compared to a regime which is limited to outsourcing core functionalities. At the end of the day, almost every contract could be "critical and important", e.g. the contract with your local energy supplier. The question is, is it meaningful and helpful to collect all this data from a regulatory perspective? And of course, from our perspective, the answer is clearly "no"!

Another important issue is interconnectedness between regulated financial entities. Is it really necessary to register contractual relations between them (while service provisions on a group level are excluded)? We think "no"! It is already difficult enough to onboard a new client or market-counterpart. We see the danger of never-ending cascading references of contractual relations. Here, we think that the AML regime strikes a right balance by acknowledging that one can usually rely on a counterpart which is obliged under the same regime to fulfill its duties.

While the draft GL state that they there shall be no overlap with DORA, it remains unclear, how firms shall handle the selection in practice. It needs at least be clarified that every service a firm considers to be DORA relevant (and handles appropriately) shall be excluded from the proposed EBA GL (with internal "DORA classification" working as a "safe harbour").

Question 3: Are Sections 5 to 10 (Title III) of the Guidelines sufficiently clear and appropriate?

Due to the lack of legal mandate discussed in question one, it is principally dispensable to address questions two to five in terms of content. Therefore, if we still make selected comments on single topics, we would like to emphasise upfront that this might not be misinterpreted as a relativisation of our fundamental critique of the scope and design of the overall concept as expressed in our answer to question 1.

At least the proposed provisions regarding conflicts of interest, business continuity plans and internal audit function are – where applicable – widely double regulation. The fragmentation of regulatory provisions contradicts the idea of a single rulebook and, even more important – ceteris paribus – harms the effectiveness and resilience of the regulatory framework.

Question 4: Is Title IV appropriate and sufficiently clear?

Due to the lack of legal mandate discussed in question one, it is principally dispensable to address questions two to five in terms of content. Therefore, if we still make comments on selected topics, we would like to emphasise upfront that this might not be misinterpreted as a relativation of our fundamental critique of the scope and design of the overall concept as expressed in our answer to question 1.

Here, we see a significant overlap with the ESMA principles addressed at NCAs (and therefore again double regulation). This might result in a conflict of competence not only between EBA and ESMA but also with the NCAs. Financial regulators and even more financial entities as addressees of financial regulation, should not be left in limbo "whose baby is it". Aside from this the ESMA principles and the proposed EBA GL differ significantly with respect to the amount of prescriptive detail (EBA) vs principle-based regulation (ESMA).

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

Due to the lack of legal mandate discussed in question one, it is principally dispensable to address questions two to five in terms of content. Therefore, if we still make selected comments on single topics, we would like to emphasise upfront that this might not be

misinterpreted as a relativisation of our fundamental critique of the scope and design of the overall concept as expressed in our answer to question 1.

As mentioned before, we se no legal basis for such a comprehensive monitoring and control, with respect to our members in particular tested with respect to investment services. Altogether, the Annex gives clear evidence of legally not mandated, overregulation. Such wide reaching intervention, while it would show a very limited or no regulatory benefit, would – even more – clearly require a Level I mandate.