Frankfurt,
8 October 2025

BVI[1] position paper on the consultation paper on EBA draft guidelines on the sound management of third-party risk

In general, we are very concerned about the proposals made by the EBA in the consultation paper on draft guidelines on the sound management of third-party risk with regard to the principle of proportionality and the lack of a legal mandate to establish such detailed documentation requirements.

Our members are affected by the consultation as investment management companies within the meaning of Directive 2009/65/EC (UCITS Directive) or Directive 2011/61/EU (AIFMD) if they are part of a banking or investment firm group. We also represent investment firms covered by the IFD and IFR framework directly if they provide investment services such as portfolio management, investment advice, reception and transmission of orders in relation to one or more financial instruments or execution of orders on behalf of clients without a licence to hold client money or securities belonging to clients or to deal on own account.

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

We reject the subject matter and scope of the draft guidelines for the following reasons:

- **Subject matter:** The draft guidelines are not in line with the European Commission's stated goal of simplifying the European legal framework and burden reduction. Extending the scope of the existing EBA outsourcing guidelines to all non-ICT third-party arrangements and not just outsourcing arrangements or services supporting critical functions will result in considerable additional work without considering the principle of proportionality. This is especially true when additional and extensive obligations (e.g. DORA-like registration requirements) are also linked to this broad scope of application. Apart from the lack of a legal basis for such far-reaching documentation requirements, we cannot see any benefit in relation to the considerable implementation effort and the stated objective of the IFD to simplify the regulatory framework. We also refer to our answer to question 3 of the consultation.

- **Lack of cooperation with ESMA**: According to Article 26(4) IFD, the EBA is expressly required to cooperate with ESMA in drawing up guidelines under the IFD framework. It appears that it has not done so in this case (at least, the consultation paper contains no indication of this; moreover, the EBA is the sole sender of the consultation). In addition, ESMA itself has already issued principles on third-party risks supervision. These ESMA principles are much more principle-based with a main focus on critical activities. Furthermore, ESMA's principles do not require the maintenance of a register, especially not for all agreements with third parties. The EBA's proposals therefore contradict ESMA's previous approaches. In our view, therefore, there is no need for further specific

[1] BVI represents the interests of the German fund industry at national and international level. The association promotes sensible regulation of the fund business as well as fair competition vis-à-vis policy makers and regulators. Asset managers act as trustees in the sole interest of the investor and are subject to strict regulation. Funds match funding investors and the capital demands of companies and governments, thus fulfilling an important macro-economic function. BVI's 116 members manage assets of EUR 4.6 trillion for retail investors, insurance companies, pension and retirement schemes, banks, churches and foundations. With a share of 26%, Germany represents the largest fund market in the EU. BVI's ID number in the EU Transparency Register is 96816064173-47. For more information, please visit www.bvi.de/en.

BVI
Bundesverband Investment und Asset Management e.V.

Contact
Phone +49 69 15 40 90 0
www.bvi.de

BVI Berlin
Unter den Linden 42
10117 Berlin

BVI Brussels
Rue Belliard 15–17
1040 Bruxelles

BVI Frankfurt
Bockenheimer Anlage 15
60322 Frankfurt am Main

Executive Board
Thomas Richter CEO
Rudolf Siebel MD

requirements, as ESMA has already set out its expectations of the relevant supervisory authorities in its principles. If the EBA does indeed wish to develop specific guidelines on the sound management of third-party risks under the IFD framework in addition to ESMA's principles, it should be done separately from the requirements for credit institutions under the CRD in close consultation with ESMA and in line with the principles already adopted by ESMA.

- **Scope of application for investment firms:** We request that the rules on sound management of third-party risk under the CRD and the IFD be strictly separated. As ESMA has already issued principles on that topic, we propose that investment firms within the meaning of the IFD be excluded from the scope of application altogether.

  We acknowledge that the EBA, in cooperation with ESMA, is mandated under Article 26(4) of the IFD to develop guidelines on internal governance, in particular on effective processes to identify, manage, monitor and report the risks that investment firms are or might be exposed to, or the risks that they pose or might pose to others. The EBA and ESMA have already done so (cf. guidelines on internal governance under Directive (EU) 2019/2034). Processes for dealing with third-party risks can already be derived today from the principles set out there.

  In any case, the EBA lacks the mandate to issue such far-reaching documentation and registration requirements for third-party risks as proposed under the new consultation paper that are comparable to the requirements for an information register under the DORA framework. According to Article 28(9) of the DORA Regulation, the ESAs are expressly mandated to develop technical implementing standards to establish the standard templates for an information register. Such a mandate is expressly absent from the IFD. Nor can we see that there is a regulatory gap in this regard or – as expressly addressed by the European Commission to the ESAs at the time via the Fintech Action Plan 2018 with regard to rules on ICT services – a need for the ESAs to draw up guidelines.

  Moreover, the previous EBA outsourcing guidelines had only a limited scope of application with regard to investment firms as defined by the CRR at the time. Certain investment firms that are not authorised to deal on their own account, do not have access to client money and only provide certain MiFID services (e.g. portfolio management) were not covered by the guidelines (because they did not qualify as institutions in the meaning of the CRR). The EBA is now extending the scope to all Class 2 investment firms, which will result in significant implementation measures, particularly for those investment firms that were not previously covered by the EBA guidelines and are now classified as Class 2 investment firms.

- **Scope of application - group regulation for asset managers with UCITS or AIFM authorisation as a subsidiary in a banking group (Art. 109 CRD) or in an investment firm group (Art. 25 IFD):** Due to the sector-specific special rules for the delegation of tasks and functions in the AIFMD and UCITS Directives, the old EBA outsourcing guidelines already led to considerable practical difficulties in the group context in the past, as the Level 3 measures laid down by the EBA are not compatible with the legal requirements for delegation arrangements in Article 20 AIFMD and Article 13 of the UCITS Directives. Unfortunately, the EU legislator has so far only recognised sector-specific special provisions in connection with remuneration rules in Article 109 CRD, but not in relation to governance rules. As this is clearly an oversight on the part of the legislator, who failed to take into account that asset managers are also subject to sector-specific governance rules under the AIFMD and UCITS Directive, a pragmatic approach should be set out

in the EBA guidelines until the oversight is remedied at Level 1. We therefore suggest a clarification in the new guidelines that in these cases the parent entity should ensure that asset managers as subsidiary undertakings, not themselves subject to the CRD or IFD, shall comply with their sector-specific requirements including ESMA's principles on third-party risks supervision.

- **Definitions**: Discrepancies between the definitions in the EBA guidelines and DORA should be avoided at all costs. This applies in particular to the definition of a critical or important function and the definition of subcontracting. Otherwise, this could lead to duplication of effort, with companies having to review their functions in accordance with both DORA requirements and EBA guidelines. This would result in a disproportionate amount of work without improving the management of third-party risk. Furthermore, no additional subcontracting should be taken into account for non-ICT-related services. We cannot see the added value here.

Question 2: Is Title II appropriate and sufficiently clear?

Scope of agreements covered and extension of the exceptions in paragraph 32 (and in the Annex) of the guidelines: It should be clarified that all supervised services between supervised entities are not non-ICT third-party services. This would be consistent with the approach taken by the ESAs and the European Commission under DORA.

Moreover, a principle-based approach should be introduced here, whereby the company at least has an overview of the contracts that support critical and important functions. Distinguishing between services that support critical and important functions and those that do not, and on top of that further distinguishing whether this constitutes outsourcing, involves an unjustifiable amount of effort. This applies to contractual requirements or documentation obligations, which have been significantly tightened in comparison to the existing EBA outsourcing guidelines. The extension of the regulations, which previously only applied to outsourcing arrangements, to other external purchases that are associated with a significantly lower risk and are not covered by DORA, leads to considerable additional burden and costs for the companies. Therefore, other services that are not essential for the performance of supervised services from a risk perspective should be excluded.

Specifically, we propose that at least the following exceptions be included in paragraph 32:

- functions which, pursuant to Article 20 of the AIFMD and Article 13 of the UCITS Directive, may be delegated by asset managers to third parties in accordance with the requirements specified therein
- cases where financial entities provide non-ICT services to other financial entities in connection to their supervised financial services
- ancillary services provided by an entity, depending on whether such ancillary services are regulated financial services or a service inseparable from, indivisible from, preparatory or necessary for the provision of a regulated financial service, and are not provided in a standalone manner

Clearer guidance should be provided to facilitate the distinction between whether a service covering several functions should be classified as an ICT service under DORA or as a non-ICT service. Ultimately, every service provider uses ICT services that are at least indirectly used for service provision. These include, for example, office communication services, online meeting platforms, office applications, and payroll and financial accounting applications. It should therefore be clarified that such ICT services that are not directly related to the service provider's service provision do not need to be

taken into account when determining whether a service is an ICT service or a non-ICT third-party service.

Furthermore, it should be clarified that ancillary services, such as the provision of the service provider's reporting system via a customer portal, do not result in the overall service being considered an ICT service in accordance with DORA.

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

- **Business continuity plans (paragraphs 55 – 58 of the drafted guidelines):** The requirements lead to considerable effort in relation to all contracts, without any apparent benefit. Therefore, if at all, they should only apply to services that are necessary for time-critical activities and processes.

- **Documentation requirements (paragraphs 61 – 69 of the drafted guidelines):** As mentioned in question 1, we strongly disagree with the proposed far-reaching documentation requirements for establishing a DORA-like register for all non-ICT third-party agreements. We cannot see any benefit in relation to the considerable implementation effort. This applies initially regardless of the type of contract to which it is to apply. A more principle-based approach should be adopted here, whereby companies are required to monitor their contracts, if necessary, but without specific requirements as to the form and identifiers used to document the respective contracts in a register.

  Irrespective of this, the proposed extension of the scope of application compared to the previous EBA outsourcing guidelines will lead to a significant increase in the administrative burden associated with maintaining the existing register, which is limited to outsourcing. It is already part of proper business organisation for a company to have an overview of its contracts with third-party providers and to take any risks into account. For the purposes of risk management and supervision of entities, such a detailed register for all third-party arrangements is not appropriate. The requirements should be reduced to an absolute minimum, namely to contracts that do not support critical or important functions.

  If there are special documentation requirements for individual contracts, it should not be necessary to make a separate distinction as to whether an outsourcing relationship also exists. Outsourcing is already subject to special requirements, most of which are sector-specific (e.g. notification requirements). The EBA guidelines should therefore not be overloaded with these issues, especially if they also directly or indirectly interfere with other sector-specific frameworks (e.g. due to group regulations or under the IFD).

  Furthermore, the proposals regarding the content of the register for non-ICT-related agreements deviate significantly from the register requirements under the DORA Regulation. This will also lead to considerable additional costs for companies, as new complex IT solutions would have to be created to implement the various requirements in a single register.

  Finally, we do not consider it appropriate to keep contracts that have already been terminated in a register.

Question 4: Is Title IV of the Guidelines appropriate and sufficiently clear?

Here, too, we suggest aligning the requirements with those of the ESMA principles and pursuing a more principle-based approach.

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

We request that the list of activities covered in the Annex I be critically reviewed once again in light of the activities excluded from the scope of application listed in paragraph 32 of the drafted guidelines in order to avoid any overlap. This applies in particular to travel services and secretarial services, which appear in both lists, making it unclear to users what actually applies with regard to these services.

****