FIA EPTA
EUROPEAN PRINCIPAL TRADERS ASSOCIATION

FIA EPTA response to the EBA Consultation on its draft Guidelines on the sound management of third-party risk (Deadline 8 October 2025)

1.Introduction

The European Principal Traders Association (FIA EPTA) represents Europe's leading Principal Trading Firms. Our members are independent market makers and providers of liquidity and risk-transfer for markets and end-investors across Europe and the UK. FIA EPTA works constructively with policy-makers, regulators and other market stakeholders to ensure efficient, resilient and trusted financial markets in Europe.

FIA EPTA welcomes the opportunity to comment on the EBA's draft guidelines on the sound management of third-party risk (the 2025 Guidelines). We note that these revised guidelines have extended the 2019 guidelines to all Class 1 minus and Class 2 investment firms (previously outside the scope), and to all third-party agreements (beyond outsourcing agreements) with some part of DORA and related RTS reproduced.

Note that the whole FIA EPTA submission has been entered in question 1, although the comments are also relevant for question 2, question 3, question 4 and question 5.

FIA EPTA members support robust risk management across the financial sector and appreciate the EBA's efforts to support ongoing enhancements to the sector's operational resilience. However, we have significant concerns regarding the proposed 2025 Guidelines with respect to the legal basis, proportionality, the misalignment with EU commission's simplification and growth agenda and the appropriateness of the EBA Costs Benefits Analysis (CBA) in particular in respects to the costs to operationalise these prescriptive and onerous requirements (e.g. such as the contractual requirements and register of information). In particular:

1) None of the legislative provisions cited by the EBA (such as the CRD, IFD, and MiFID II references noted above) empower the imposition of a comprehensive DORA-style regime covering all non-ICT related services provided by a third-party service provider (TSPS) to financial entities in the EU. Such provisions are high level and broad in nature, and cannot reasonably amount to a valid mandate for a regime that seeks to mirror the extensive and granular requirements established under DORA.

If EU legislators had intended to introduce DORA-style regulation to cover all forms of outsourcing and third-party service provision in the financial sector, not just those related to digital operational resilience, they would have provided a specific mandate for this purpose. This would mirror the formal legislative process followed for DORA, where a clear and valid mandate was obtained from the EU Parliament and Council.

This ultimately undermines the confidence of market participants in the legislative process (blurring the boundary between supervisory guidance and quasi legislation) and undermines the authority of the Commission as sole legislative power.

2) In light of the principle of proportionality laid down in Article 5(4) of the Treaty on European Union the, EBA has not clearly articulated why the imposition of a highly prescriptive and burdensome framework of requirements (i.e. a DORA-like regime imposed through Level 3 guidance) is a proportionate measure that achieves the objective (of ensuring adequate oversight of third-party non-ICT risks) via the least burdensome measure available in relation to the objective being sought. The EBA has not identified any significant or newly emerging risks to the financial sector (which have emerged since 2019) that relate to arrangements with non-ICT third-party service providers (i.e. TSPS) and that are comparable to the third-party ICT risks addressed by DORA, nor has the EBA identified material gaps in existing sectoral requirements (e.g. MIFID II Delegated Regulation and IFD) that may create a risk for financial stability

3) These guidelines undermine the Commission's simplification and competitiveness agenda, diverging from the commission strategic priorities, weakening the EU unified voice on simplification, growth and competitiveness. This misalignment risks questioning the credibility of the Commission's agenda.

In line with the EU simplification agenda, it is FIA EPTA's view that the EBA should further the objective of proportionality and regulatory simplification by limiting the updates of these 2025 Guidelines to what was strictly required to strengthen financial stability arising from material gaps under the existing 2019 guidelines, or under sectoral requirements (e.g. CRD, IFD, MIFID II DR), have been identified. In this respect, the EBA should have either excluded all class 2 firms already subject to more suited sectoral regulations or at the very least should have taken a more risk based and outcome focused approach by only extending the guidelines to i) those class 2 investment firms that have a material impact on the market or consumers (and not including all class 2 firms particularly those in class 2 based on a zero threshold), AND to ii) material third party arrangements that support a critical and important function (as assessed by the financial entity). In addition the EBA should have excluded services provided by regulated entities to align with DORA (ESA Q&A1) and prevent unnecessary double supervision.

Finally, FIA EPTA strongly disagrees with the EBA's CBA statement (which is not substantiated at all) that the revised guidelines will have low impact due to the existing detailed sectoral directives Investment firms are subject to. Indeed, existing sectoral frameworks applicable to investment firms (MIFID II Delegated Regulation and IFD) are principles and outcome based and better reflect the operational realities and the risks that investments firms pose to the market or consumers. We therefore expect the cost to operationalise these 2025 Guidelines for investment firms to be significant (adding to the significant costs already incurred from DORA implementation) and more importantly, disproportionate to the benefits (standardisation). We see an increasing material disconnect between the EBA and the industry's impact assessment that needs to be addressed.

We therefore urge the EBA to exclude class 2 firms that are already subject to more proportionate and appropriate sectoral regulations (e.g. MIFID II DR) or consider realigning the 2025 Guidelines with a more risk based and outcome focused approach in line with the existing sectoral framework applicable to investment firms (e.g. MIFID II DR), and in line with the approach taken by other jurisdictions such as the approach taken in the UK by the PRA's 'Supervisory Statement on Outsourcing and third party

[1] Q74 ESA Q&A: in case a financial entity must be authorised/licenced/registered as financial entity to deliver a service, such service is therefore a regulated financial service and not an ICT service in the meaning of DORA Article 3(21).

risk management'. At the very least, we urge the EBA to introduce meaningful proportionality by focusing on material risks and material TPSPs only.

We set out our concerns in further detail below.

2. Legal Basis and Proportionality

Legal Basis

FIA EPTA notes that the 2025 Guidelines expressly seek to replicate and align with Regulation EU 2022/2554 (DORA) and its associated mandates. For instance, the EBA notes the following at section 2(7) (Subject matter, scope and definitions) of the 2025 Guidelines (emphasis added):

"The management of information and communication technology (ICT) risk and the use of TPSPs to provide ICT services as defined in Article 3(21) of Regulation EU 2022/255425 (DORA) are not under the scope of application of these Guidelines as they fall under the scope of DORA. In this regard, these Guidelines only cover the use of TPSPs providing or supporting functions that are not qualified as ICT services under DORA. Consistency has been ensured, to the extent possible with DORA and its relevant mandates; while DORA provides for the framework on the management of third-party risks with regard to ICT services, those Guidelines apply for non-ICT related services provided by TPSPs."

FIA EPTA has concerns around the appropriateness of imposing a DORA-style regime exclusively through Level 3 measures (namely, in the form of a 46-page guidance document). The DORA regime is comprised of an overarching regulation (i.e. Level 1 legislation), which is directly binding on all Member States and was established following a robust legislative process involving the EU Commission, Parliament and Council – and which resulted in express Parliamentary and Council approval for the regime. The DORA Level 1 text is complemented by various delegated and implementing acts (i.e. Level 2 measures), which the EU Commission has been specifically empowered to adopt under the DORA Level 1 mandate.

By contrast, the 2025 Guidelines currently seek to rely solely on various broad, high-level and varied provisions across a number of regulations / directives – none of which expressly empower or contemplate the imposition of a DORA-like regime across the financial services sector.

By way of example, the following enabling provisions are cited in the 2025 Guidelines:

- Directive 2013/36/EU **(CRD)**

Article 74(3) CRD states the EBA shall "issue guidelines on the arrangements, processes and mechanisms" referenced in Article 74(1).

Article 74(1) CRD specifies that institutions in scope of CRD "shall have robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks they are or might be exposed to, adequate internal control mechanisms, including sound administration and accounting procedures, and remuneration policies and practices that are consistent with and promote sound and effective risk management."

Aside from the above (which the EBA considers encompasses third-party arrangements)2 there is no specific prescription in CRD empowering the creation of a DORA-style framework for all non-ICT services procured by financial entities in scope of CRD.

- Directive 2019/2034/EU (**IFD):**

Article 26(4) IFD states that the "EBA, in consultation with ESMA, shall issue guidelines on the application of the governance arrangements" referenced in Article 26(1).
Article 26(1) IFD requires Member States to ensure that investment firms have "*robust governance arrangements, including all of the following: (a) a clear organisational structure with well-defined, transparent and consistent lines of responsibility; (b) 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; (c) adequate internal control mechanisms, including sound administration and accounting procedures; (d) remuneration policies and practices that are consistent with and promote sound and effective risk management.*"

Aside from the above, there is no specific prescription in IFD empowering the creation of DORA-style framework for all non-ICT services procured by investment firms in scope of IFD.

- Directive 2014/65/EU (**MiFID II**) and Commission delegated regulation (EU) 2017/565 supplementing MiFID II (**MiFID II Delegated Regulation)**

MiFID II and the MiFID II Delegated Regulation prescribe organisational requirements for investment firms.

Under Article 16(5) of MiFID II, investment firms must take reasonable steps to avoid undue operational risk for "the performance of operational functions which are critical for the provision of continuous and satisfactory service to clients and the performance of investment activities on a continuous and satisfactory basis".

Additionally, under Article 16(5) of MiFID II, the "outsourcing of important operational functions" may not be undertaken in a way that impairs a firm's internal control or ability of a supervisor to monitor the firm's compliance with its obligations.

For these purposes, an "*outsourcing*" is defined under Article 2(3) of the MiFID II Delegated Regulation as "*arrangement of any form between an investment firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the investment firm itself*", which is in line with the definition adopted by the EBA Guidelines on Outsourcing Arrangements (2019) (**the 2019 Guidelines**).

Furthermore, "*an operational function shall be regarded as critical or important where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under Directive 2014/65/EU, or its financial performance, or the soundness or the continuity of its investment services and activities*" as per Article 30(1) of the MiFID II Delegated Regulation.

Accordingly, MiFID II is concerned only with the outsourcing of critical or important functions. Neither MiFID II nor the MiFID II Delegated Regulation provide for requirements to be imposed on any other types of outsourcing arrangements, or requirements for the provision of third-party services more widely – and there is no accompanying mandate in MiFID II for the EBA to impose requirements on this basis.

[2] Section 2 (*Executive Summary)* of the EBA's consultation.

Additionally, the EBA refers to Article 16 of Regulation (EU) No 1093/201013 (the EBA Regulation) which states the following at paragraph 1 (emphasis added):

The Authority shall, with a view to establishing consistent, efficient and effective supervisory practices within the ESFS, and to ensuring the common, uniform and consistent application of Union law, issue guidelines and recommendations addressed to competent authorities or financial institutions. Guidelines and recommendations shall be in accordance with the empowerments conferred by the legislative acts referred to in Article 1(2) or in this Article."

Notably, Article 16(1) of the EBA Regulation refers only to the issuance of guidelines and recommendations to support the common, uniform and consistent application of existing Union law. Additionally, the adoption of guidelines must be in accordance with the nature of the empowerments conferred under the relevant legislative acts.

None of the legislative provisions cited by the EBA (such as the CRD, IFD, and MiFID II references noted above) empower the imposition of a comprehensive DORA-style regime covering all non-ICT related services provided by a third-party service provider (TSPS) to financial entities in the EU.3 Such provisions are high level and broad in nature, and cannot reasonably amount to a valid mandate for a regime that seeks to mirror the extensive and granular requirements established under DORA.

If EU legislators had intended to introduce DORA-style regulation to cover all forms of outsourcing and third-party service provision in the financial sector – not just those related to digital operational resilience – they would have provided a specific mandate for this purpose. This would mirror the formal legislative process followed for DORA, where a clear and valid mandate was obtained from the EU Parliament and Council.

In the absence of a specific EU legislative mandate empowering the extension of DORA (or the creation of a new DORA-style regime) to cover all non-ICT service providers to the financial sector, it would be inappropriate to rely on the provisions above to impose requirements that are not otherwise contemplated under Union law.

Proportionality

FIA EPTA is concerned that the 2025 Guidelines, as currently drafted, do not adequately respect the principle of proportionality to which the EBA is required to adhere under the EBA Regulation, specifically Article 1(5) and Article 8(3).

The principle of proportionality is laid down in Article 5(4) of the Treaty on European Union and requires that measures taken by EU institutions (emphasis added):

(i) must be suitable to achieve the desired end;
(ii) must be necessary to achieve the desired end; and
(iii) must not impose a burden that is excessive in relation to the objective sought to be achieved.

The case law of the Court of Justice of the European Union (CJEU) further clarifies that, where there is a choice between appropriate measures, competent authorities should select the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued.

[3] As per the scope noted in section 2 (*Executive Summary)* of the EBA's consultation, and section 2 (*Subject matter, scope and definitions)* of the 2025 Guidelines.

With respect to the 2025 Guidelines, the EBA has not clearly articulated why the imposition of a highly prescriptive and burdensome framework of requirements (i.e. a DORA-like regime imposed through Level 3 guidance) is a proportionate measure that achieves the objective (of ensuring adequate oversight of third-party non-ICT risks) via the least burdensome measure available in relation to the objective being sought. Furthermore, and as further detailed below, the EBA's cost benefit analysis does not provide a sufficiently thorough consideration of the costs of compliance associated with the 2025 Guidelines, in a manner that would justify the extensiveness of the measures being imposed. With respect to the proportionality of the 2025 Guidelines as a whole, the EBA merely notes the following:

"*To cater for the principle of proportionality, the Guidelines require to identify the provision of critical or important functions by third-party service providers (TPSPs) to financial entities and Impose stricter requirements compared with other third-party arrangements*."[4]

In FIA EPTA's view, the EBA has not provided a sufficiently clear or compelling articulation of the risks posed to the financial sector by existing TSPS relationships nor of potential gaps in existing sectoral regulations or frameworks, which would necessitate a response that is mostly equivalent to the regime imposed by DORA. This is particularly important given that DORA sought to address the largely unique and novel risks posed by the rapid acceleration of ICT service usage in the financial sector since the Covid-19 pandemic. The introduction of DORA reflects the increased digitalisation and digital interconnectedness in the financial sector, which was assessed to have amplified ICT risks and made "the financial system in particular, more vulnerable to cyber threats of ICT disruptions" (see Recital 1 DORA).

The EBA has not identified any significant or newly emerging risks to the financial sector (which have emerged since 2019) that relate to arrangements with non-ICT third-party service providers (i.e. TSPS) and that are comparable to the third-party ICT risks addressed by DORA, such as cybersecurity threats or cyber-attacks. Given the absence of an equivalent level of risk, extending the detailed and onerous requirements of DORA to non-ICT risk providers would be both inappropriate and disproportionate (particularly in the absence of empowering Level 1 legislation).

The EBA could have, and should have, limited the updates of these guidelines to what was strictly required to strengthen financial stability when material gaps under the existing 2019 guidelines, or under sectoral requirements (e.g CRD, IFD, MIFID II DR), have been identified. In this respect, the EBA could have either excluded all class 2 firms already subject to more suited sectoral regulations or at the very least could take a more risk based and apply meaningful proportionality:

1) by including only investment firms that have a material impact on the market or consumers (and not including all class 2 firms particularly those in class 2 based on a "zero" threshold). In particular as it is today, an investment firm trading on own account with 1 employee and holding 1 share worth 1 Euros would have to apply the 46 pages of guidelines AND
2) by including only material third party arrangements that support a critical or important function (CIF). In particular, Class 2 firms should be required to carry out a materiality assessment to determine which of their TSPS (which fall outside the scope of DORA) support the Class 2 firm's CIFs. This assessment should be in line with the applicable definition and test in MiFID II, which specifies that an operational function is a CIF where a defect or failure in its performance would materially impair: (i) the firm's continued compliance with its authorisation conditions or other requirements under MiFID II, (ii) its financial performance, or (iii) the soundness or continuity of

[4] Section 5.1(B) (*Accompanying documents: Draft cost-benefit analysis/impact assessment*) of the EBA's consultation.

its investment services and activities.5 Where the materiality impact assessment carried out by the Class 2 firm concludes that the TSPS is supporting a CIF, then it would be appropriate to apply the extensive requirements in the 2025 Guidelines. Where the TSPS is not supporting as CIF (e.g. because the TSPS provides purely routine, ancillary or standard administrative functions), then the application of the full suite of extensive 2025 Guidelines would be disproportionate to the low level of risk posed by the TSPS. In such instances, the Class 2 firm would nevertheless continue to comply with the existing core requirements in the MiFID II DR with respect to such TSPS (i.e. adequate record-keeping, appropriate due diligence and contractual provisions, and ongoing supervision).This proposed approach would be in line with the approach taken by the Prudential Regulation Authority (PRA) in the UK for banks and systemically important investment firms (which also applies third party risk requirements based on a similar materiality assessment to the one outlined above).6 It would thereby ensure that the EU does not impose a substantially more onerous set of requirements on moderate-sized investment firms (i.e. Class 2 firms) compared to the UK regulatory framework, which would create further compliance costs and competitive disadvantages for establishments in the EU.

3) By excluding services provided by regulated financial entities in line with DORA as clarified in a recent Q&A7

Cooperation with ESMA

Under Article 26(4) of the IFD, the EBA is expressly required to cooperate with the European Securities and Markets Authority (ESMA) when drafting guidelines with respect to the governance requirements under Article 26(1) IFD. It is unclear whether such cooperation has taken place with respect to the proposed 2025 Guidelines.

In particular, FIA EPTA notes that ESMA has already issued a set of principle-based guidelines for the oversight of third-party risks (notwithstanding that those guidelines were addressed to NCAs only) – and that such guidelines omit a number of the prescriptive and granular requirements (e.g. an information register) that the 2025 Guidelines are now seeking to impose. This appears to indicate a discrepancy in supervisory approach between the EBA and ESMA.8

3. PRACTICAL IMPACT OF THE EBA GUIDELINES TO INVESTMENT FIRMS REGULATED UNDER IFR/IFD

Taking into account the breath of these requirements, FIA EPTA focuses its submission on highlighting the far reaching impact of these 2025 Guidelines on investment firms and ask the EBA either to exclude class 2 firms already subject to more suited sectoral regulations, or to consider realigning the 2025 guidelines more closely to the existing MIFID II DR. At the very least, the EBA should increase meaningfully the proportionality of the requirements by focusing on material risks and material TPSP only.

The EBA 2019 Guidelines on Outsourcing (the **2019 Guidelines**) were applicable to certain investment firms under the CRR until the IFR came into force, defining several classes of investment firms. Since

---

5 Article 30(1) of the MiFID II Delegated Regulation.

6 Please see Chapter 5 ("Materiality Assessment") of PRA Supervisory Statement on Outsourcing and third party risk management | SS2/21.

7 Q74 ESA Q&A: in case a financial entity must be authorised/licenced/registered as financial entity to deliver a service, such service is therefore a regulated financial service and not an ICT service in the meaning of DORA Article 3(21).

8 ESMA 'Principles on third-party risks supervision' (12 June 2025).

the introduction of the IFR, Class 2 investment firms have been outside the scope of the EBA Guidelines and are instead subject to the MiFID II outsourcing delegated regulation 2014/65/EU (the MiFID II DR).

When comparing with the 2025 Guidelines, we note that the MiFID II DR set a more proportionate and appropriate set of requirements, that are more fit-for-purpose to Class 2 investment firms, while still being comprehensive in terms of scope. In contrast, the 2025 Guidelines, in aggregate result in requirements that would be excessively burdensome for investment firms, and (as set out in the section above) without any clear articulation as to the granular risks that EBA seeks to mitigate. We note the desire to harmonise approach to the DORA regulations. However, the proposal lacks analysis demonstrating why DORA should serve as the template for all third-party risk management. The EBA has not articulated the specific risks these changes are intended to address, nor substantiated why a treatment similar to DORA is necessary. Consequently, this appears to be harmonisation for its own sake, with insufficient regard for the implementation costs Class 2 investment firms will face and with no assessment of which incremental risks the 2025 Guidelines would additionally mitigate beyond those already adequately managed under existing requirements.

The key ways in which the MiFID II DR delivers more proportionate and fitting outcomes include (as further detailed below):

- Focuses upon the outsourcing of Critical and Important Functions (CIFs) themselves
- Does not automatically pull into scope ancillary services that support CIFs
- Does not prescribe any format of a register of information, but does require firms to maintain adequate records
- Requires key and proportionate contractual provisions be in place for CIFs, but does not require extensive contractual changes across all contracts with third parties
- Takes a more appropriate and proportionate approach to inter-affiliate service provision.

Below we further detail why the proposed 2025 Guidelines constitute an unnecessarily onerous change to the existing MiFID DR particularly with regard to Class 2 investment firms, and the reason why we ask that that EBA consider each element in turn when reassessing the cost-benefit analysis of the proposed 2025 Guidelines and consider realigning the 2025 guidelines more closely to the existing MIFID II DR or at least increase meaningfully the proportionality of the requirements.

a. Scope

The most material difference between the 2025 Guidelines and both the 2019 Guidelines and MiFID II DR is that 2025 Guidelines extends to all TSPS with very limited exception. By contrast:

- The 2019 Guidelines apply only to outsourcing of functions that could "*realistically be performed by institutions or payment institutions, even if the institution or payment institution has not performed this function in the past itself.",*
- The MiFID II DR only applies to outsourcing of "*critical or important functions*" (**CIF**) themselves (and does not automatically include services that support those functions).

Both the 2019 Guidelines and MiFID II DR take a far more proportionate and pragmatic approach to scoping. It remains unclear and is not examined at all in the cost benefit analysis attached to the 2025 Guidelines, what firm, client, or market risk the EBA is looking to address by extending the scope to all TPSPs. For example, the 2025 Guidelines would bring into scope a contract with a personnel background screening provider (an HR service provider), and all market data contracts would fall into scope of the 2025 Guidelines (unless already captured by DORA). In both cases, firms terminate and enter into new contracts with such types of providers regularly with little operational risk, and without the need to implement extensive contractual changes required in the 2025 Guidelines. By contrast,

the approach of the MiFID II DR is far more pragmatic and risk based, by focusing only on where investment firms outsource CIFs to third parties (e.g. compliance, risk management) and where there is clear potential risk.

We welcome the carve-out for services without material impact on risk or operational resilience (Title 2, 3.3). However, the EBA's examples (e.g., gardening, architecture) are completely disconnected from the financial services context and would risk creating the impression that unlisted ancillary financial services are automatically caught. We urge the EBA to either clarify by setting out clear, outcomes-oriented principles to differentiate material from non-material risk areas, or at least confirming the list is non-exhaustive or removing it entirely, allowing firms to focus resources on arrangements with genuine material risks.

The 2025 Guidelines do not currently exclude regulated financial services that are provided to firms that are in scope for the 2025 Guidelines. We note that regulated financial services are already subject to extensive requirements relating to their provision as are the firms that provide them. We struggle to see what additional risk mitigation is achieved by requiring one regulated firm to apply the 2025 Guidelines to another regulated firm that is already directly subject to those same Guidelines. We further note that DORA recognized the limited benefit of such a requirement and for this reason the ESAs exempted regulated financial services from its scope.

We believe that either a reversion to the approach under the MiFID II DR, or an increased degree of proportionality to determine contracts that are material (as also detailed in the proportionality section), is required. The EBA may want to adopt the more proportionate approach taken by the PRA as also referred to in the proportionality section.

b. Definitions

Where previously the 2019 Guidelines used the term function to refer quite clearly to a firm's internal functions and only its internal functions, in the 2025 Guidelines functions now refer to any services provided to a firm as noted in the definition of Third-Party arrangement, which includes "….the provision of one or more functions to the financial entity". As a result of how the definition of function now operates in the 2025 Guidelines, it also means that the definition of Critical and Important Function is not aligned with DORA. While in DORA Critical and Important Functions clearly related to a firm's own internal functions, similar to how the term was used in the 2019 Guidelines (functions are internal to the entity, services may or may not support those functions). In the 2025 Guidelines, Critical or Important Function includes any service from a third party that meets the criteria for critical or important. This is a significant change from the definition in DORA ie. from an internal activity that may be supported or provided by a third party to any service from a third party. As such the changes do not bring greater alignment with DORA as intended by the EBA, but instead result in substantial disjunction between the two.

In addition, many sections of the 2025 Guidelines blur these two concepts: sometimes a TSPS is characterised as performing the part or all of an internal function for a firm (in line with the 2019 Guidelines) and, in others, the 2025 Guidelines instead use the concept simply to mean the service being provided. The 2025 guidelines would be clearer if the term function was used, as it is in DORA and the 2019 Guidelines, to refer specifically to the internal functions of a firm and the defined term third-party arrangement should refer to the provision of services to the firm, that may or may not support a critical or important function. This would bring better alignment with DORA but would also avoid various points where the use of the term is ambiguous in the 2025 Guidelines.

c. Inter-affiliate Service Provision

The MiFID II DR takes a far more proportionate approach on the use of affiliates for the provision of critical functions than the 2025 Guidelines. It states[9]: "*Where the investment firm and the service provider are members of the same group, the investment firm may, for the purposes of complying with this Article and Article 32, take into account the extent to which the firm controls the service provider or has the ability to influence its actions.*"

We would urge the EBA to consider this approach to reduce the regulatory burden on firms. Requiring firms to treat intra-group services under the same framework as external third-party providers creates significant additional administrative burden. This burden is unjustified: Intra group arrangements have shared ownership and control which vested interest, aligned strategic interests, greater transparency and oversight and integrated operational policies processes. While not free from risk, these features reduce the risk of operational failure. In addition, the firm retains ultimate responsibility for services provided by affiliates, making the duplicative oversight requirements unclear in purpose and disproportionate in cost.

The MiFID II DR ensures that control and responsibility is retained by the EU regulated firm which should be sufficient to reduce the operational burden attached to such intra-group outsourcing, a setup which is incredibly common in the industry and should not require detailed administrative requirements inclusive of the need for detailed contractual requirements between affiliates and for such relationships to be documented in a detailed register of information.

d. Governance

On governance, both the MiFID II DR and 2019 Guidelines take a far more proportionate approach as compared to the 2025 Guidelines. The 2019 Guidelines' governance requirements attach to outsourced services only rather than to any TPSP. The 2019 framework is therefore more targeted (as it involves fewer third-party relationships) and more effective in delivering the objective of protecting firms from operational risk and ensuring firms maintain oversight over their own core functions that they may have decided to outsource.

While FIA EPTA fully accepts that firms should have processes and procedures for managing third party service providers, the significantly prescriptive nature of the 2025 Guidelines, and their lack of substantive clear proportionality imposes risks significant administrative burdens for unclear benefit. As noted elsewhere in this reply it is unclear why firms require a policy to manage all of their TPSPs. If such relationships are sufficiently numerous, firms will have procurement teams with their own policies and procedures in place designed specifically for the firm, its business practices, its TSPS and the risks they pose, and not limited to the highly prescriptive requirements in the 2025 Guidelines.
These Guidelines both lack of risk sensitivity (as they are not appropriate for all firms) and are too prescriptive (as again, their level of prescriptiveness is not appropriately tailored to the risks TSPS pose to EU markets or consumers).

The MiFID II DR takes a much more proportionate and outcome based approach to governance. Like the 2019 Guidelines, the more effective scope helps ensure that governance requirements are focused on only those TPSP relationships that pose material risk to firms, and by imposing expectations rather than prescriptive conditions on firms, MiFID II allows firms to manage their TPSP in a way which works for the organisation whilst ensuring that firms remain "*fully responsible for discharging all of their obligations*" and that "*the outsourcing does not result in the delegation by senior management of its responsibility".*

[9] Article 31(4) if the MIFID II DR

In the context of the SIU where the EU Commission clearly indicated its strategic objectives to support simplification by reducing regulatory burden and unnecessary red tape (ensuring rules and regulations are fit for purpose and do not unduly burden firms with unnecessary or unproven administrative requirements), it is hard to see how these guidelines, which are unnecessarily prescriptive and lack crucially of proportionality, contribute to the burden reduction and simplification's objectives. The EBA could have taken a different approach and retained the risk based and outcome based approach similar to the MIFID II DR.

e. Register of Information

The proposal in the 2025 Guidelines for the TPSP register is, alongside the extended scope of these guidelines, one of the most concerning aspects of the guidelines. The EBA's proposal to use the DORA template for tracking TPSPs significantly underestimates the substantial administrative burden and complexity of the DORA register requirements. We strongly urge the EBA to reconsider this approach, as it risks imposing highly disproportionate requirements on firms that are in no way commensurate with the actual risks being managed. It should be recalled that the DORA register contains almost 100 fields across 14 tabs which would need to be completed for each TPSP (and replicated down all the subcontracting chains, including where affiliates are involved). This is more than five times as many as the registers suggested by the 2019 Guidelines (up to 18 fields). Moreover, the MiFID II DR takes the even more outcomes based approach of allowing firms to apply their own TPSP tracking approaches based on their risk management framework.

We further note that firms are not only subject to MiFID II record keeping requirements but also to corporate law and accounting record keeping requirements, which means that all investment firms would already be tracking all their TSPS. While it is important to ensure firms have a record of their TSPS and are able to access key details of those providers from their record keeping systems, it is hard to see what further risk reduction is gained by requiring firms to maintain such information in a separate register outside of their contractual database systems. Before imposing such a requirement on firms, we would urge that the EBA to clarify whether there have in fact been any substantive risks posed by firms' current TSPS database management processes, and if so, which sorts of firms and what specific risks.

It is unclear on the face of the 2025 Guidelines cost benefit analysis what evidence the EBA has for requiring a register for all TPSPs. In the case of DORA, firms only produced the register of information to comply with the requirements and, to our knowledge, no FIA EPTA member firms find it helpful for any form of risk management or useable as a tool for contract management, noting as well that in its submitted xbrl-xml format (ie. unreadable), it is largely unusable for such purposes.

f. Contractual Requirements

The 2025 Guidelines further add to the regulatory burden with prescriptive contractual requirements which are significantly more detailed than either the MiFID II DR or the 2019 Guidelines. The EBA has not adequately assessed the significant costs firms will face in changing (and renegotiating) existing contracts to meet these new requirements. The cost-benefit analysis fails to justify this burden by demonstrating what specific risks would be reduced. Before imposing contractual changes or repapering that will require substantial legal, operational, and commercial resources across potentially hundreds of third-party relationships, the EBA must conduct a rigorous assessment of actual implementation costs and clearly articulate the corresponding risk mitigation benefits. Again, we note that MiFID II DR takes a more pragmatic and proportionate approach, appreciating that firms may

determine the most appropriate contractual arrangements with counterparties in order to ensure the continuity of the CIFs being outsourced. It remains unclear why this approach is not sufficient nor has the EBA articulated what supervisory risks have crystallised from a lack of specific contractual clauses with TPSPs.

It is for example unclear what concrete operational risk the EBA seeks to address by prescribing that contracts explicitly state where services are being provided and where data is being stored. These provisions in the 2025 Guidelines will require firms to add to pre-existing contracts clauses which wouldn't typically appear in a contract – these details would typically be agreed commercially between parties and it is unclear why they need to be in formal contracts. We further note that, as a general rule, if the contracts relate to personal data, such matters will already have been addressed under GDPR. And where they relate to a firm's own sensitive data, this is a matter that most firms have every incentive to handle in a way that aligns to their interests and data management policies and requirements.

It is similarly unclear what risk is being addressed by having detailed exit and termination contractual provisions prescribed by the draft guidelines. Any firm operating in a commercial environment will ensure it has appropriate and robust termination rights in their contracts and to have the ability to exit more material contracts without exposing itself to operational risk. Firms should be left to negotiate these provisions in the form that works for them and is commercially pragmatic rather than needing such provisions to match a template laid down by these draft guidelines. Again, we note that the MiFID II DR took a far more effective approach in having outcomes-based requirements rather than prescriptive requirements for outsourced contracts.

It should be noted, in this regard, that DORA contractual (re)negotiations have consumed many months of firms' resources, with many negotiations still ongoing. We note that the EBA has not provided any post-implementation analysis demonstrating that DORA's substantial administrative burden in this area delivered proportionate benefits. Firms have incurred significant legal, operational, and commercial costs renegotiating contracts. Before extending similar requirements through the 2025 Guidelines, we reiterate that the EBA should provide clear evidence that these burdens produce meaningful risk reduction. Without such evidence, imposing equivalent contractual requirements would be clearly disproportionate

4. EBA Costs Benefits Analysis and Simplification

The EBA Costs Benefits Analysis (CBA) states that the revised guidelines will have low impact due to existing sectoral directives that already establish a set of requirements for outsourcing that is quite detailed. FIA EPTA strongly disagree with this assessment which is also not substantiated at all.

As explained in more detail above, existing regulatory requirements applicable to investments firms (MIFID II DR and IFD 26 together with the IFD guidelines on internal governance) in respect of third-party risk management and outsourcing are significantly less prescriptive and are significantly more outcome and principle based. In particular, although the MIFID II DR does require firms to maintain adequate records and mandate key and proportionate contractual provisions to be in place for CIFs, the requirements do not automatically pull into scope ancillary (i.e. non material) services that support CIFs, do not to prescribe any format of a register of information and do not require extensive contractual changes across all contracts with third parties. The DR MIFID II requirements applicable to investment firms therefore materially depart from the proposed 2025 Guidelines which will no doubt create a material administrative burden.

The work to renegotiate all in scope contracts alone is a significant, material additional compliance requirement, the costs and time required for which should not be minimized or disregarded. Similarly, while all firms subject to MIFID II will have record retention systems that ensure they can maintain and monitor existing contractual arrangements, those systems may not be able to generate a databased that tracks exactly the requirements set forth in the 2025 Guidelines for the register of information. In particular, the requirements set out in 63.a, 63.g, 63.h and even 63.k, as DORA implementation has indicated, do not neatly fit onto firm's existing contract arrangements or how third-parties themselves understand and manage the services they provide, resulting in significant time and effort to obtain this information from other TSPS. While we understand that the register requirements in the 2019 Guidelines was leveraged for DORA as being most similar and so a sensible base off of which the DORA register of information could be based, we would urge the EBA to consider whether all of the various fields are in fact particularly relevant in the context of all third party contracts, as many are not. This is an area where either more explicit proportionality or divergence from the 2019 Guidelines and DORA seems more appropriately calibrated to the risks and burdens involved in the register requirements.

Although investment firms would have in place third party risk management frameworks, these would not be standardised but rather adapted to the size and business model of the firm, and aligned with the sectoral frameworks applicable to investment firms which reflect better operational realities and the risks that these firms pose to itself, the market or consumers.

This CBA therefore significantly underestimates the cost of standardisation as well as the cost of operationalising 46 pages of extensive and prescriptive requirements for class 2 investment firms that were not previously subject to the 2019 Guidelines.

We would like the EBA to address specifically this point in its response to the consultation paper and in particular to provide more detail on the methodology used to perform this CBA. Taking into account the material discrepancy in impact assessment between the industry and the EBA, it is likely that no practitioner from the industry provided input and contributed to this CBA. Should it be the case, FIA EPTA question how regulators can be confident the CBA is a realistic reflection of the potential costs of new regulation if it hasn't spoken with industry practitioners. This questions the governance process of the CBA, which needs urgently to be reviewed and improved.

Finally, as mentioned elsewhere in this submission, it is our belief that the current guidelines undermine the Commission agenda of simplification and competitiveness. Not only are the requirements disproportionate, not risk based, and arguably not necessary as explained in much detail above, firms have to spend a lot of resources to do a line-by-line comparison with the existing 2019 guidelines and the DORA wording to identify whether the language is aligned. As an example, it is not clear in para - Para 43 (g) and (h)- whether the governing body needs to review the TPSP's BCP and audit, or whether the governing body needs to review the financial entity's BCP and audit in respect of the 1/3 P arrangement. Comparing this wording with DORA in Art 5 it seems that the words "financial entities" have been omitted in these guidelines which can have a material impact on the scope of the requirements. While we would welcome clarification on this point, the broader point is that the EBA should have performed a thorough review of the drafting throughout the entirety of the 2025 Guidelines and, if it is to expect firms to understand how these 2025 Guidelines differ from other similar regulation, it should have provided the industry with a blackline version comparing the 2019 and 2025 Guidelines and with a DORA gap analysis.