# AEIP Position on the Digital Operational Resilience Act

17 May 2021

European Association of Paritarian Institutions - AEIP

## Key messages on DORA

- Institutions for Occupational Retirement Provision (IORPs) are inherently different from other financial market entities in the sense that they are 'not-for-profit', play an important social role in pension adequacy, they don't have any shareholders and most importantly don't sell products, since employees often benefit from a mandatory affiliation to the pension scheme on the basis of their employment relationship. Second pillar pension schemes often have a paritarian structure, meaning that they are set up and managed jointly by social partners, while additional costs are borne either by the organizers of the scheme, by increasing their pension contributions, or by the employees, by way of a reduction in their benefits. It is also important to stress that the IORP landscape among EU Member States is very heterogeneous in terms of scale, type of pension scheme, social and labour law, institutional design as well as contractual obligations. In that regard, IORPs do not compete with same type financial entities in different Member States, making them less relevant to be included in the scope of the DORA Regulation. Moreover, these specificities of IORPs necessitate a more principle-based approach and better reflection of the proportionality principle in legislative proposal, as we will explain in more detail in our position.
- Provident institutions of social protection[1] are also inherently different from other financial market entities. They are 'not-for-profit' organizations and manage collective health insurance contracts established by collective agreements between social partners. Importantly, they are paritarian in structure, thus being operated by employers and employees on a joint basis. These specificities, which are shared with IORPs, call as well for a principle-based approach and an appropriate implementation of the proportionality principle in DORA.
- The IORP II Directive sets clear requirements regarding governance and risk management, including those on operational and ICT risk as well as outsourcing. These rules, which are specific for the IORP environment and have proven effective in practice, should prevail on these similar requirements as introduced by DORA. But also in regard to provident institutions of social protection, the Solvency II Directive recognizes ICT risks as a component of operational risks so these are already part of the integrated risk management system of provident institutions and are taken well into account in capital requirements, governance and reporting. To that end, it should be explicitly indicated in the text that the DORA Regulation applies insofar that the specific regulatory framework to which the financial entity is subject to on a national or European level, does not provide any specific provisions to limit the ICT risks of this financial entity.
- The current low yield environment makes IORPs and provident institutions sensitive to any additional fixed costs, on top of the already existing investment costs, administration costs, governance costs and communication costs. We fear that mainly small and medium-sized IORPs and provident institutions will be highly negatively impacted by the required measures, since

[1] Provident institutions of social protection (Institutions de prévoyance) are not-for-profit organizations that manage collective health insurance contracts, which are established within the exclusive framework of the company or sectoral collective agreement. These contracts cover the risks of illness, incapacity for work and invalidity, as well as dependency or death. Provident organizations are legally governed by the French Code of Social Security (and as such comply with European Directives on insurance, including the Solvency II Directive). Please see more here: https://ctip.asso.fr/ctip/les-ip-et-les-gps/

these lead to fixed costs and proportionality for small and medium-sized IORPs is mainly lacking in the text. Eventually, such an impact will have detrimental effects on the retirement income of members and beneficiaries, thus impeding the significant social role of IORPs. Thus, the requirements of the DORA Regulation should not impose significant additional burden and should have a much more proportional approach to the IORPs' ICT risk.

- We believe it is necessary to make a distinction between these IORPs that outsource all operational activities and those that don't. In particular, for IORPs which outsource all operational activities the Regulation should only focus on the provisions for managing the ICT third party risk.
- Introducing proportionality by referring to microenterprises as well as small and medium-sized enterprises alone without their specific context is not the right approach, since the classification of small, medium or large entities should refer to the specific environment or sector of the respective financial entity. As proportionality is of the utmost importance in this context, each type of financial entity needs its own 'sectoral' reference point. For example, an IORP, whose main goal is managing pension savings will by definition have higher turnover and/or balance sheet totals than most small and medium-sized enterprises in general. As a consequence, for IORPs we believe that only staff headcount should be taken into account in this context, disregarding the financial ceilings given that these amounts are not a good measure for determining the size of IORPS. Importantly, as also stated in the European Parliament's ECON Committee amendment proposal, micro, small or medium-sized IOPRs and provident insurers should be excluded from the Regulation's scope.
- In regard to ICT risk management we suggest to refer much more to commonly used and proven business standards like ISO or Cobit to align the requirements with good practices existing on the market.
- Given that the creation of a centralised database for incident reporting will entail additional reporting requirements for IORPs and provident institutions of social protection-on top of the existing various reporting requirements- there is no added value in the creation of an extra superfluous system, in addition to the systems already in place that comply with national and international standards.
- Instead of developing new standards, provisions on classification and reporting of ICT-related incidents should rather be aligned with existing international standards and good practices.
- Regulatory overload should be avoided while coordination between institutions is a very important aspect, given that the current DORA proposal overlaps to a great extent with other regulatory outputs at the EU level, such as EIOPA's guidelines on outsourcing to cloud service providers as well as its guidelines on ICT security and governance.
- Under the current regulatory framework of IORP II and Solvency II Directive, all operational and ICT risks as well as compliance costs are eventually borne by IORPs and provident institutions respectively. In that regard, any effort to enhance the monitoring of third-party providers and outsourced service providers should take into consideration this fact and rather aim to ease the burden for these non-for-profit financial entities.
- In order to enhance proportionality, we should ensure that existing contracts do not need to be adapted immediately right after the Regulation's coming into force. Instead, when the Regulation enters officially into force, existing contracts can be kept unchanged and respected until their termination date, so all new contracts should be in line with these new requirements.

**Horizontal approach of introducing regulative requirements in the financial sector is detrimental for the majority of IORPs across the EU as well as for provident institutions of social protection, which are small and medium-sized.**

We would like to stress that IORPs are different from any other financial entity in the sense that they don't have any shareholders, are 'not-for-profit' and do not sell products, since employees often benefit from a mandatory affiliation to the pension scheme given their employment relationship. Second pillar pension schemes are set up and managed jointly by social partners and additional costs are borne either by the organizers of the scheme, by increasing their pension contributions, or by the employees, by way of a reduction in their benefits. It is also important to stress that the IORP landscape across the EU is very heterogeneous in terms of scale, type of pension scheme, social and labour law, institutional design as well as contractual obligations. Nevertheless, most IORPs in the EU are small in terms of size, which means that often they do not even have their own personnel, so they use sponsor resources and outsource -sometimes all of- their operational and investment services. Provident institutions of social protection are also inherently different from other financial market entities. They are 'not-for-profit' organizations and manage collective health insurance contracts established by collective agreements between social partners. Notably, they are paritarian in structure, thus being operated by employers and employees on a joint basis. The current low yield environment makes both IORPs and provident institutions sensitive to any additional fixed costs, on top of the already existing investment costs, administration costs, governance costs and communication costs. Due to all the above, we believe it is crucial that the specificities of these two types of institutions are better reflected in the DORA requirements and these can benefit from a more proportional treatment in this context, thus not jeopardizing their important societal goal in providing adequate pension income as well as healthcare and long-term care benefits to their members and beneficiaries.

One of the arguments the European Commission uses as an underlying rationale for this legislative initiative is the following, as stated in Recital (9): *"Legislative disparities and uneven national regulatory or supervisory approaches on ICT risk trigger obstacles to the single market in financial services, impeding the smooth exercise of the freedom of establishment and the provision of services for financial entities with cross-border presence. Competition between the same type of financial entities operating in different Member States may equally be distorted."*

This might be an argument for numerous financial entities, however not for IORPs and provident institutions, which only execute and manage an agreement made by social partners. In a sense, they manage schemes which are not in competition. Therefore, one could argue that IORPs and provident insurers should not be in scope of this Regulation as the "competition distortion argument" does not apply and from a governance and risk perspective many of these measurements are already imposed by the IORP II Directive [Directive (EU) 2016/2341] and the Solvency II Directive [Directive (EU) 2009/138/EC].

**Link with the IORP II Directive and Solvency II Directive**

From the perspective of IORPs and provident institutions of occupational social protection, the DORA legislative proposal introduces additional regulatory requirements on top of the existing framework, given that many requirements have been already introduced in one way or another by the IORP II Directive and the Solvency II Directive.

We therefor strongly disagree with the following reasoning, as mentioned in the context of the proposal: *"The absence of detailed and comprehensive rules on digital operational resilience at EU level has led to the proliferation of national regulatory initiatives (e.g., on digital operational resilience testing) and supervisory approaches (e.g., addressing ICT third-party dependencies). Action at Member State level, however, only has a limited effect given cross-border nature of ICT risks. Moreover, the uncoordinated national initiatives have resulted in overlaps, inconsistencies, duplicative requirements, high administrative and compliance costs - especially for cross-border financial entities - or in ICT risks remaining undetected and hence unaddressed. This situation fragments the single market, undermines the stability and integrity of the EU financial sector, and jeopardises the protection of consumers and investors. It is therefore necessary to put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities. This framework will deepen the digital risk management dimension of the Single Rulebook. In particular, it will enhance and streamline the financial entities' conduct of ICT risk management, establish a thorough testing of ICT systems, increase supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities, as well as introduce powers for financial supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers. The proposal will create a consistent incident reporting mechanism that will help reduce administrative burdens for financial entities and strengthen supervisory effectiveness."*

We believe this reasoning not be correct. Indeed, various Member States have already introduced different requirements on operational resilience taking into account their respective national approach of operational activities. Given the fact that this Regulation comes "on top" and that there isn't any initiative to replace the existing requirements, this will by definition lead to additional administrative burden and an increase in fixed costs.

In light of the specific context of IORPs, which are mainly small or medium-sized across the different EU member states and which need to operate in a "lower for longer" environment, cost control is essential to ensure their business continuity. Given that IORPs already have comprehensive risk management in place, including operational and ICT risk, but also given that they outsource most or even all of the operational activities due to their lack of scale, any additional extra burden should be limited at all costs, and the requirements introduced by DORA should be much more in proportion to the ICT risk of IORPs. In regard to provident institutions of occupational social protection, the Solvency II Directive, recognizes ICT risks as a component of operational risks (see Art. 13 No. 33 of SII). Thus, these risks are already part of the integrated risk management system of provident institutions and are taken well into account in capital requirements, governance and reporting.

In this context we suggest:

- to refer to IORP II Directive and Solvency II Directive as much as possible, as this specific legislation takes more into account the characteristics of a provident institution and of an IORP (not for benefit, executing an agreement of social partners, paritarian management, in most of the cases no pan-European activities, etc…);

- to make a distinction between IORPs that outsource all operational activities and those that don't. For those IORPs that outsource all operational activities the focus should be on managing the ICT third party risk as described in Chapter V of the legislative proposal. At financial entity level the IORP II Directive requirements regarding the governance and risk management of operational risk should be sufficient (see IORP II Directive: article 20 – responsibility of the management or supervisory body, 21 – general governance requirements, 25 – risk management 28 – own risk assessment, 31 -outsourcing).
- The prevailing legislation (i.e. IORP 2016/2341 and Solvency II 2009/138) provides, by its nature of Directives, some flexibility to Member States to get adapted. DORA, in its nature of Regulation, would not provide such leeway.

## Proportionality

Member States stressed the need to ensure proportionality and consider the specific situation of small companies or subsidiaries of larger groups. In the context description of the DORA proposal the following was included: *"The proposed rules do not go beyond what is necessary in order to achieve the objectives of the proposal. They cover only the aspects that Member States cannot achieve on their own and where the administrative burden and costs are commensurate with the specific and general objectives to be achieved. Proportionality is designed in terms of scope and intensity through the use of qualitative and quantitative assessment criteria. These aim to ensure that, while the new rules cover all financial entities, they are at the same time tailored to risks and needs of their specific characteristics in terms of their size and business profiles. Proportionality is also embedded in the rules on ICT risk management, digital resilience testing, reporting of major ICT-related incidents and oversight of critical ICT third-party service providers."*

Furthermore, in the proposal text the European Commission acknowledges the fact that significant differences exist between financial entities in terms of size, business profiles or in relation to their exposure to digital risk. Nevertheless, we believe that the call of the Member States to ensure proportionality in the DORA proposal was not sufficiently reflected in the text. In particular, the proposal text lacks proportionality in several ways:

- Due to the horizontal approach, the specific characteristics of the financial entities are totally ignored, as also mentioned earlier.
- Financial entities that outsource all their operational activities seem to be required to put an entire detailed framework in place. We believe that for those entities the DORA requirements should be limited to managing the ICT third party risk.
- Financial entities are very heterogeneous in nature across national markets as well as across Europe. Even more so, IORPs present a diverse landscape, with some of them managing less than € 10 million in pension provisions while others manage amounts of up to € 400 billion or more.
- IORPs do not "sell" products, they execute and manage an agreement made between social partners. This requires much more proportionality and a more principle-based approach. We suggest to refer much more to commonly used and proven business standards like ISO (e.g. ISO 27005 on Information security risk management) or Cobit to align the requirements with good practices existing on the market. Furthermore, any system of incident reporting must align with industry standard reporting frameworks such as Mitre Att&ck.

- Introducing proportionality by only referring to microenterprises as well as small and medium-sized enterprises is not the right approach. An IORP, whose main goal is managing pension savings will by definition have higher turnover and/or balance sheet totals than most small and medium-sized enterprises in general. Instead, the classification of small, medium or large entities should refer to the specific environment of the respective financial entity. As proportionality is of the utmost importance in this context, each type of financial entity needs its own 'sectoral' reference point. As a consequence, for IORPs we believe that only staff headcount should be taken into account in this context, disregarding the financial ceilings given that these amounts are not a good measure for determining the size of IORPS. Importantly, as also stated in the European Parliament's ECON Committee amendment proposal, micro, small or medium-sized IOPRs and provident insurers should be excluded from the Regulation's scope.

## Cost impact

The cost impact of this proposal is huge, especially for small and medium-sized IORPs but also for provident institutions. The proposal's introduction recognizes that the retained option would give rise to costs of both one-off and recurring nature, by stating the following: *"The one-off costs are mainly due to investments in IT systems and as such are difficult to quantify given the different state of firms' complex IT landscapes and in particular of their legacy IT systems. Even so, these costs are likely to be limited for large firms, given the significant ICT investments they have already made. Costs are also expected to be limited for smaller firms, as proportionate measures would apply given their lower risk."*

As proportionality for small and medium-sized IORPs is totally lacking and as the required measures all induce fixed costs, we fear that mainly small and medium-sized IORPS, and thus their members and beneficiaries, will be substantially impacted by these measures in a negative way. In this context, it should be stressed that a 1% extra cost over a duration of 25 years results in either a 25% reduction of the benefits for members and beneficiaries or a 25% cost increase for the sponsoring undertaking, or a combination thereof. IORPs have already in place specific risk measures, including measures on operational and ICT risks. Any extra measures should only be considered after performing a thorough cost/benefit-analysis and should be implemented only if they really represent an added value.

It should be noted that apart from the substantial cost increase linked to these additional measures as mentioned above, the DORA Regulation will also bring about additional costs for the supervisory authorities which in turn will be transferred to the financial entities under their supervision.

We would also like to stress that under the current regulatory framework of IORP II and Solvency II Directive, all operational and ICT risks as well as compliance costs are eventually borne by IORPs and provident institutions respectively. In that regard, any effort to enhance the monitoring of third-party providers and outsourced service providers should take into consideration this fact and rather aim to ease the burden for these non-for-profit financial entities, and finally to lower the costs for their beneficiaries.

Finally, regulatory overload should be avoided while coordination between institutions is a very important aspect, given that the current DORA proposal overlaps to a great extent with other regulatory outputs at the EU level, such as EIOPA's guidelines on outsourcing to cloud service providers as well as its guidelines on ICT security and governance.

## Detailed remarks on the DORA Proposal

**Summary overview**

| ***Chapter*** | ***Section*** | ***Article*** | ***Subject*** | |
|---|---|---|---|---|
| *I General Provisions* | | *1* | *Subject matter* | *-* |
| | | *2* | *Personal scope* | *Referring to the existing specific regulatory framework to which the financial entity is subject to on a national or European level in order to enhance proportionality and limit administrative burden and excessive costs.* |
| | | *3* | *Definition* | *Amending the scope of the Regulation for insurance undertakings and IORPs as follows:*<br><br>*Art. 2, par. 1 (o): institutions for occupational retirement provision unless they are micro, small or medium-sized enterprises*<br>*Art. 2, par. 1 (m): insurance and reinsurance undertakings, unless they are micro, small or medium-sized enterprises and do not rely on systematised insurance intermediation*<br><br>*Amending definition of 'microenterprises' as well as 'small and medium-sized enterprises' for IORPS in the sense that only staff headcount should be taken into account to determine enterprise categories (disregarding the financial ceilings since the indicated amounts are not a good* |

| | | | | |
|---|---|---|---|---|
| | | | | *measure for IORPS in determining their size).* |
| *II ICT Risk Management* | *I* | *4* | *Governance and organisation* | *Introduction of a distinction between financial entities that outsource all critical operational activities (including ICT services to run their business operations) and those that don't* |
| | *II* | *5* | *ICT Risk management framework* | *There should be no digital resilience strategy for microenterprises and small and medium-sized enterprises.*<br>*More emphasis should be given on proportionality: due consideration to their size, business and risk profiles*<br>*More exemptions for micro, small and medium-sized enterprises.*<br>*Possibility of outsourcing.* |
| | | *6* | *ICT systems, protocols and tools* | |
| | | *7* | *Identification* | |
| | | *8* | *Protection and prevention* | |
| | | *9* | *Detection* | |
| | | *10* | *Response and recovery* | |
| | | *11* | *Backup policies and recovery methods* | |
| | | *12* | *Learning and evolving* | |
| | | *13* | *Communication* | *There shouldn't be any communication policies for staff and for external stakeholders for microenterprises as well as small and medium-sized* |

| | | | | |
|---|---|---|---|---|
| | | | | *enterprises, nor designation of a specific person within the financial entity tasked with implementing the communication strategy.* |
| | | *14* | *Further harmonisation of ICT risk management tools, methods, processes and policies* | *-* |
| *III ICT-RELATED INCIDENTS MANAGEMENT, CLASSIFICATION and REPORTING* | | *15* | *ICT-related incident management process* | *Not mandatory in case financial entities already have an ICT-related incidents management system in place that is compliant with national or international standards. No need to create a superfluous system on top of systems which are already in place. Input needed for the creation of a European registry should be collected from the national competent authorities (based on the national incident-reporting they receive). Possibility of outsourcing.* |
| | | *16* | *Classification of ICT-related incidents* | |
| | | *17* | *Reporting of major ICT-related incidents* | |
| | | *18* | *Harmonization of reporting content and templates* | |
| | | *19* | *Centralisation of reporting of major ICT-related incidents* | |
| | | *20* | *Supervisory feedback* | |
| *IV DIGITAL OPERATIONAL RESILIENCE TESTING* | | *21* | *General requirements for the performance of digital operational resilience testing* | *Not mandatory in case financial entities already have a basis testing system in place that is compliant with national or international standards and could be sector-specific.*<br>*Possibility of outsourcing. Any initiative in this field should follow a risk-based approach and respect the principle of proportionality.* |
| | | *22* | *Testing of ICT tools and systems* | |
| | | *23* | *Advanced testing of ICT tools, systems and* | *-* |

| | | | | |
|---|---|---|---|---|
| | | | *processes based on threat led penetration testing* | |
| | | *24* | *Requirements for testers* | *-* |
| *V MANAGING OF ICT THIRD-PARTY RISK* | *I KEY PRINCIPLES FOR A SOUND MANAGEMENT OF ICT THIRD PARTY RISK* | *25* | *General principles* | *It is crucial to establish adequate transitional provisions in the sense that the new provisions will only come into effect upon renewal of the contractual arrangements (sort of 'grandfathering').*<br>*Promote standard clauses*<br>*The current list of key contractual provisions is over-prescriptive; we should try to alleviate the most stringent provisions.* |
| | | *26* | *Preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements* | |
| | | *27* | *Key contractual provisions* | |
| | *II OVERSIGHT FRAMEWORK OF CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS* | *28* | *Designation of critical ICT third-party service providers* | *-* |
| | | *29* | *Structure of the Oversight Framework* | *-* |
| | | *30* | *Tasks of the Lead Overseer* | *-* |
| | | *31* | *Powers of the Lead Overseeer* | *-* |
| | | *32* | *Request for information* | *-* |
| | | *33* | *General investigations* | *-* |
| | | *34* | *On-site inspections* | *-* |
| | | *35* | *Ongoing Oversight* | *-* |
| | | *36* | *Harmonisation of conditions enabling the conduct of the Oversight* | *-* |

| | | | | |
|---|---|---|---|---|
| | | *37* | *Follow-up by competent authorities* | *-* |
| | | *38* | *Oversight fees* | *-* |
| | | *39* | *International cooperation* | *-* |
| | | *37* | *Follow-up by competent authorities* | *-* |
| | | *38* | *Oversight fees* | *-* |
| | | *39* | *International cooperation* | *-* |
| *VI INFORMATION SHARING ARRANGEMENTS* | | *40* | *Information-sharing arrangements on cyber threat information and intelligence* | *-* |
| *VII COMPETENT AUTHORITIES* | | *41* | *Competent authorities* | *-* |
| | | *42* | *Cooperation with structures and authorities established by Directive (EU) 2016/114* | *-* |
| | | *43* | *Financial cross-sector exercises, communication and cooperation* | *-* |
| | | *44* | *Administrative penalties and remedial measures* | *-* |
| | | *45* | *Exercise of the power to impose administrative penalties and remedial measures* | *-* |
| | | *46* | *Criminal penalties* | *-* |
| | | *47* | *Notification duties* | *-* |

| | | | | |
|---|---|---|---|---|
| | | *48* | *Publication of administrative penalties* | - |
| | | *49* | *Professional secrecy* | - |
| *VIII DELEGATED ACTS* | | *50* | *Exercise of the delegation* | - |
| *IX TRANSITIONAL AND FINAL PROVISIONS* | | *51* | *Review Clause* | - |
| | | *52* | *Amendments to Regulation (EC) No 1060/2009* | - |
| | | *53* | *Amendments to Regulation (EU) No 648/2012* | - |
| | | *54* | *Amendments to Regulation (EU) No 909/2014* | - |
| | | *55* | *Amendments to Regulation (EU) No 600/2014* | - |
| | | *56* | *Entry into force and application* | - |

**AEIP Disclaimer**

AEIP represents the European Paritarian Institutions of Social Protection in Brussels since 1997. The Association gathers 27 leading large and medium-sized Social Protection Management Organizations which equally represent the employees and the employers through a joint governance scheme; plus 39 affiliates from 22 countries

AEIP represents its members' values and interests at the level of both European and International Institutions. In particular, AEIP - through its working groups - deal with EU coordinated pension schemes, pension funds, healthcare schemes, unemployment schemes, provident schemes and paid holiday schemes.

Owing to the quality of its members and to the delegation of powers conferred to its Board, AEIP aims at becoming the leading body for the promotion of balanced paritarian social protection systems in Europe. AEIP promotes and develops programs and orientations aiming at the sustainability of paritarian social protection systems at local level taking into account the national specificities aiming at ensuring social cohesion in Europe.

Based thereon, AEIP prepares recommendations, proposes local programs and influences European decisions to safeguard and promote the interests of its members. AEIP thinks ahead and anticipate modern paritarian social protection systems that take into account changing economic and societal pattern. It furthermore seeks to find a new balance between and across generations.