Digital Operational Resilience Act (DORA)

Why does it matter to intermediaries?

The Digital Operational Resilience Act (DORA) is part of the Commission's Digital Finance Strategy that was published in September 2020. DORA's primary objective is to enhance the IT security of financial entities. DORA will aim to establish a comprehensive digital operational resilience framework across the European banking, insurance and investment sectors, requiring financial entities in its scope to comply with digital security and reporting requirements to mitigate their information communication technology (ICT) risks.

Insurance intermediaries who are SMEs and microenterprises are exempted from the scope of DORA and its level 2 measures. Opt-out investment firms under MiFID II are exempted as well. Larger insurance intermediaries are in scope. It is possible, however, that under certain circumstances insurers (or clients) will require (partial or full) DORA compliance of service providers (such as intermediaries) at national level.

DORA entered into force on 16 January 2023 and will start applying - together with its level 2 measures - on 17 January 2025. The Regulation is binding in its entirety and directly applicable in all Member States.

Financial entities in the scope of DORA will have to respect strict common standards to ensure they can withstand ICT- related disruptions and threats. They will have to put in place, amongst others:

- dedicated ICT risk management capabilities (contract compliance, as part of 'ICT Third-Party Risk Management' is one of the five pillars of DORA),
- harmonised reporting of major ICT-related incidents,
- digital operational resilience testing,
- management by financial entities of ICT third-party risk,
- information sharing among financial entities.

DORA also introduces some key principles for a sound management of ICT third party risks as well as an EU oversight framework for critical ICT service providers (such as Big Techs which provide cloud computing to financial institutions).

DORA has assigned new tasks and roles to the ESAs, as well as the development of a set of policy mandates before DORA enters into application, i.e. the drafting of Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) on certain provisions of the DORA Regulation:

- RTS on ICT risk management framework,
- RTS on simplified ICT risk management framework,
- RTS to further specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by third-party providers (TPPs),
- RTS to specify elements when sub-contracting critical or important functions,
- two RTS on incident reporting,
- ITS to establish the templates for the Register of information and,
- by 30.09.2023, the input to the Commission's Call for advice on criticality criteria.

RTS and ITS of the ESAs aim to clarify the provisions of a European legislative text and to ensure a coherent harmonisation of the defined areas. All of the above-mentioned RTS and ITS will be of importance for intermediaries falling under the scope of DORA and having to comply with it. For example, the ESAs' RTS specifying which elements to be included in the ICT security policies, procedures and protocols referred to in DORA to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse.

State of play

DORA level 2 measures

The DORA Regulation mandates the European Supervisory Authorities (EIOPA, ESMA and EBA – the ESAs) to develop a series of level 2 measures to complement/specify the level 1 requirements (see above). Over the last year, the ESAs conducted two consultations on their draft proposals for these level 2 measures. BIPAR responded to these consultations. Following these consultations, the ESAs reviewed the comments received from stakeholders and adjusted the draft level 2 measures accordingly.

On 17 January 2024, as announced during the webinar BIPAR organised with EIOPA on the issue on 16 January**, the ESAs published their final reports on some of the draft level 2 measures** and **sent them to the European Commission for adoption**.

In March 2024, based on the ESAs' proposals, the Commission adopted the following level 2 measures:

- **Commission's Delegated Regulation** supplementing DORA with regard to RTS specifying the **criteria for the classification of ICT-related incidents and cyber threats,** setting out materiality thresholds and specifying the details of reports of major incidents,
- Commission's **Delegated Regulation** supplementing DORA with regard to RTS specifying the **detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions** provided by ICT third-party service providers,
- Commission's **Delegated Regulation** supplementing DORA with regard to RTS specifying **ICT risk management tools, methods, processes, and policies** and the simplified ICT risk management framework.

The measures will be subjected to a 3-month scrutiny period until mid-June during which time the European Parliament and the Council will be able to formulate objections. If no objections are formulated, the measures will be published in the OJ of the EU and will enter into force.

The Commission is expected to adopt the remaining level 2 measures by the end of June.

Consultation on remaining level 2 measures

On 18 April 2024, the ESAs issued a consultation paper containing a draft RTS on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1) point (c) of DORA. This consultation paper and the included draft RTS cover the draft technical standards aimed at specifying the criteria for determining the composition of the joint examination team ensuring a balanced participation of staff members from the ESAs and from the relevant competent authorities, their designation, tasks, and working arrangements. As the empowerment included in point (c) of Article 41(c) has an impact only on the supervisory community, BIPAR did not respond to the consultation.

ESAs' voluntary exercise on collection of registers of information

During a webinar organised on 30 April 2024 and in which BIPAR participated, the ESAs provided the industry with information on their voluntary exercise for the collection of the registers of information of contractual arrangements on the use of ICT third-party service providers by the financial entities (such as large insurance intermediaries).

Under DORA and starting from 2025, financial entities will have to maintain registers of information regarding their use of ICT third-party providers. In this **"dry run" exercise**, the information will be collected from financial entities through their competent authorities and will serve as preparation for the implementation and reporting of registers of information under DORA.

The ESAs and the NCAs are introducing this voluntary exercise to help financial entities prepare for establishing their registers of information, gathering the relevant information specified in the **ESAs' final draft Implementing Standards on the registers of information** and reporting them to their respective competent authorities, who will, in turn, provide them to the ESAs. The ESAs will provide individual and general feedback to financial entities regarding their registers of information in the second half of 2024.

BIPAR's position / key messages

During the legislative process

Insurance intermediaries were included in the scope of the Commission's proposal for DORA, together with much larger financial entities such as insurers or credit institutions.

While BIPAR welcomed DORA's objective to increase the digital operational resilience of the financial sector, it informed the EU legislators that the financial sector is not uniform in scale and structure. The incidents experienced by different financial services entities, as well as their consequences (for the financial stability, consumers etc.), differ from one financial services sector to another. DORA's requirements would simply not be operationally and financially sustainable for (small) insurance or financial intermediaries. DORA's regulatory architecture was not adapted to the insurance distribution sector, and BIPAR pointed out that proportionate application of its numerous and detailed requirements would be difficult to ensure in practice (further complicated by levels 2 and 3 measures).

For BIPAR and its members, insurance and financial intermediaries (and, in particular, micro and SMEs) had, therefore, to be completely exempted from DORA. This message was successfully relayed to MEPs, the Council and the Commission.

EIOPA's consultations

In its responses to the ESAs' consultations on DORA level measures, **BIPAR highlighted the importance of maintaining the proportionality and flexibility of the DORA framework**. This was reflected in the ESAs draft RTS that include recitals explaining the concept of proportionality under DORA and acknowledging the different operational structures and risk profiles of the entities in scope.

In line with BIPAR's comments, the **ESAs clarified for example certain technical requirements** regarding, inter alia encryption, administration of ICT assets, human resources policies, collection and analysis of data, business continuity plans, etc.

The ESAs also acknowledged BIPAR's point on the high complexity of the RTS. BIPAR suggested the ESAs should issue non-mandatory guidance at a later date, to provide entities in scope with more detail on how to comply with the requirements. The ESAs mention the possibility of issuing future guidance on business continuity management, amongst others.

On the classification of major ICT-related incidents, **the ESAs took into account BIPAR comments mentioning the complexity of the classification framework and simplified the process**. Regarding classification criteria and threshold, BIPAR underlined the need for flexibility in order to make the criteria and threshold relevant to all entities in scope (which vary in size, nature, risk profile, etc.). The ESAs took these comments into account and:

- increased certain thresholds, in order to avoid overreporting,
- allowed the use of estimates for certain criteria to lower reporting burden,
- clarified the scope and meaning of certain criteria,
- removed the reference to "escalation to senior management" as an indicator, in line with BIPAR's suggestion, as this would disproportionately impact smaller entities,
- exempted SMEs from having to report on "recurring incidents".

The ESAs, in line with BIPAR's comments, significantly simplified the reporting templates, removing a number of fields.

The ESAs also took into account BIPAR's comments regarded proportionality and flexibility, including the following:

- Possibility for groups to maintain a single register at the most consolidated level, rather than multiple registers depending on the group's structure,
- Streamlining of required fields,
- Removal of the requirement for an "audit functionality",
- Review "on a regular basis" rather than "ongoing".

Regarding the proposed taxonomy of ICT services, BIPAR's comments point out its complexity and its lack of clarity. The ESAs clarified a number of definitions, eliminated unnecessary elements and specified that services listed are not mutually exclusive, allowing for more precision when classifying services.

Next steps

- Adoption by the Commission of the remaining level 2 measures in the summer of 2024.
- Publication in the OJ of the EU of all DORA level 2 measures.
- DORA and its level 2 measures will apply as of 17 January 2025.
- BIPAR will be monitoring with its member associations the application of DORA in Member States.

Links

- Digital Operational Resilience Act (DORA)
- Delegated Regulation supplementing DORA with regard to RTS specifying the criteria for the classification of ICT-related incidents and cyber threats
- Delegated Regulation supplementing DORA with regard to RTS specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions
- Delegated Regulation supplementing DORA with regard to RTS specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework.
- ESAs' consultation paper on the draft RTS on the conduct of oversight activities
- ESAs' final draft Implementing Standards on the registers of information
- Commission's Digital Finance Strategy
- ESA's dry run exercise

Markets in Crypto-Assets Regulation (MiCA)

Why does it matter to intermediaries?

The MiCA Regulation will establish uniform rules across the European Union for crypto assets. It covers issuers of unbacked crypto-assets and the so-called "stablecoins", as well as the trading venues and the wallets where crypto-assets are held. The Regulation covers intermediaries when selling with advice unit-linked life insurance products with crypto-asset funds as underlying investments.

In its position on the MiCA proposal, the European Parliament amended the article on advice on crypto assets of the proposal and introduced a ban on remuneration "*paid or provided by an issuer or any third party or a person acting on behalf of a third party in relation to the provision of the service to their clients.*"

State of play

- The final text as adopted in trilogue by the Council and Parliament Plenary did not include the EP proposed general ban on remuneration. Instead, it included– as a compromise – wording that is very similar to MiFID II, namely amongst others, **a duty to inform the client if advice is provided on an independent basis**. **Where independent advice is provided, then commission is banned (also a ban on commission for portfolio management, as in MiFID II).**
- The Council of the EU officially adopted and published the MICA text on its website on 31 May 2023.
- MiCA was published on 9 June 2023 in the Official Journal of the EU.
- MiCA includes an important number of level 2 and level 3 measures (technical standards) that need to be developed by the ESAs before the new regime commences. Once finalised they will provide greater granularity on the provisions in the MiCA.
- On 25 March 2024, ESMA published:
  1) a final report on the first package of measures under the MiCA,
  2) a final report on the cooperation between various authorities in relation to the MiCA, and
  3) a consultation document on the third package of measures under the MiCA.

  Stakeholders are encouraged to provide their feedback by 25 June 2024.

BIPAR's position / key messages

BIPAR and its members informed lawmakers that they were opposed to the ban on commission as proposed by the EP and provided arguments against such a ban. As explained above, this was taken on board by the co-legislators.

Next steps

The rules will start applying on 30 December 2024 (+/- 18 months after entry into force) but with application for certain parts of the Regulation (Titles III (Asset-Referenced Tokens) and IV (E-Money Tokens) already on 30 June 2024.

Links

- MiCA Regulation
- ESMA's final report on the first package of measures under the MiCA
- ESMA's final report on the cooperation between various authorities in relation to the MiCA
- ESMA's consultation document on the third package of measures under the MiCA