BIPAR Paper

6 January 2022

DORA - Proposed Regulation on digital operational resilience for the EU financial sector
State of Affairs
Preparation for Trilogue

BIPAR Register ID number: 349128141758-58

BIPAR
Avenue Albert-Elisabeth 40
B-1200 Brussels

Tel: +32/2/735 60 48
Fax: +32/2/732 14 18
bipar@bipar.eu
www.bipar.eu

BIPAR is the European Federation of Insurance Intermediaries. It groups 47 national associations in 30 countries. Through its national associations, BIPAR represents the interests of insurance agents and brokers and financial intermediaries in Europe.

Besides some large multinationals, the insurance intermediation sector is composed of hundreds of thousands of SMEs and micro-type operators. It accounts for 0.7% of European GDP, and over one million people are active in the sector. Insurance and financial intermediaries facilitate the insurance and financial process for several hundreds of millions of customers. The variety of business models, the high level of competition and the geographical spread in the sector ensure that everyone in Europe has easy access to tailor-made insurance and financial services.

BIPAR is a member of the World Federation of Insurance Intermediaries (WFII).

I. INTRODUCTION

On 24 September 2020 the European Commission published a draft Regulation on digital operational resilience for the EU financial services sector (DORA).

According to the Commission, *the EU therefore needs to update its rules to ensure that financial-sector ICT systems can withstand security threats and that third-party ICT providers are monitored.*

The Commission proposal aims to introduce a **harmonised and comprehensive framework on digital operational resilience** for various European financial entities, including **insurers and insurance intermediaries**.

In this light, in a proposed Directive, the Commission also proposes amendments to the Solvency II, AIFM, IORPs MiFID II, PSD and prudential supervision Directives to clarify certain provisions in these existing financial services directives regarding digital resilience. No amendments to the IDD are proposed.

DORA proposal also introduces an oversight framework for critical ICT service providers (such as Big Techs) which provide cloud computing to financial entities. The European Supervisory Authorities (ESAs) will operate as Lead Overseers, and the national supervisors as enforcers. The ESAs will have the right to access documents and to carry out inspections.

According to the Commission's proposal, **DORA imposes 120 "digital checkpoints" that would apply to over 500 000 SME insurance intermediaries** in the same way as to the NYSE EURONEXT, large banks or insurers. However, 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. The incident experienced by a small intermediary with 15 employees or by a medium-sized intermediary can't be compared to an incident experienced by a large credit institution.

DORA further includes some exemptions for microenterprises, but they are too narrow as microenterprises are only exempted from a few of DORA requirements (only 10 out of the 120 requirements).

This BIPAR Paper provides a state of affairs on the EU legislative procedure regarding the DORA proposal, particularly in relation to insurance intermediaries and explains why insurance intermediaries cannot be compared with banks or insurers from a (digital) resilience perspective.

Ahead of the trilogue negotiations (between Commission, Council, EP), this Paper also illustrates that the general principle of proportionality does not work in practice and puts forward proposals for alternative routes for reflection.

BIPAR is of the opinion that it is necessary to study again the DORA proposal in all its details before insurance intermediaries are brought into scope. Insurance intermediaries should be exempted from the scope of DORA and the digital resilience of insurance intermediaries should be examined within the framework of the IDD revision or in the framework of a future digital resilience regulation that applies to all other sectors.

In summary, BIPAR believes that:

- ✓ the 500 000 insurance intermediaries need to be attentive in terms of cybersecurity but individually do not pose a threat to the "financial stability". Every service (and production) sector in the economy should be careful and aware of cyber risks, but imposing 120 digital checkpoints on (SME) insurance intermediaries is not commensurate to the risk.
- ✓ The Commission's impact assessment has not measured the effects on and (compliance and supervision) costs of having 500 000 "traditional "insurance intermediaries in the scope of DORA.

II. KEY POINTS of Commission proposal for DORA

- **What is Digital operational resilience?**

  The digital operational resilience is defined as "*the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality".*

- **What is the scope of DORA?**

  The Commission proposal has a very broad scope and applies to many financial entities such as **insurance and reinsurance undertakings, insurance and reinsurance intermediaries as defined by the IDD**, as well as institutions for occupational retirement pensions, credit rating agencies, statutory credit institutions, payment institutions, electronic money institutions, investment firms, crypto-asset service providers, central securities depositories, CCPs, trading venues, trade repositories, AIFMs, management companies, data reporting service providers, audit and audit firms, administrators of critical benchmarks, crowdfunding service providers, securisation repositories.

  It also applies to **ICT third-party service providers. "***ICT third-party service provider" means an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, data centres, but excluding providers of hardware components and undertaking which provide electronic communication services.*
  When adopted, DORA will bring critical third-party service providers – such as cloud computing services – within a direct oversight of the European Supervisory Authorities.

- **What are the key DORA requirements?**

The proposed Regulation sets out **requirements** concerning **the security of network and information systems supporting the business processes of financial entities,** needed to achieve a high common level of digital operational resilience:

(a) requirements applicable **to financial entities** in relation to:
- Information and Communication Technology (ICT) **risk management** (Art.4-14);
- **reporting** of major ICT-related incidents to the competent authorities (Art.15-20);
- digital operational resilience **testing** (Art.21-24);
- measures for a **sound management of the ICT third-party risk** by financial entities (Art.25-26);
- information and intelligence sharing in relation to cyber threats and vulnerabilities (Art.40);

(b) requirements in relation to **the contractual arrangements concluded between ICT third-party service providers** and financial entities (Art.27);

(c) the oversight framework for **critical ICT third-party service providers** when providing services to financial entities (Art.28-39);

(d) rules on cooperation among **competent authorities and rules on supervision and enforcement** by competent authorities in relation to all matters covered by this Regulation (Art.41-39).

PLEASE SEE THE DORA REQUIREMENTS IN DETAIL IN ANNEX I.

- **How is the proportionality principle embedded in DORA proposal?**

Proportionality and risk-based application is embedded in DORA proposal; use of qualitative and quantitative assessment criteria. So financial entities, like insurance intermediaries, can in theory tailor the requirements to their specific risks and needs, **depending upon their size, business profiles, and technology risks.**

In recital (20) of DORA proposal, it is explained that "the digital operational resilience bar for the financial system should be raised **while allowing for a proportionate application of requirements for financial entities which are micro enterprises** as defined in Commission Recommendation 2003/361/EC."

In its recital (33) of DORA proposal, it is explained that "*Notwithstanding the broad coverage envisaged by this Regulation, the application of the digital operational resilience rules should take into consideration* ***significant differences between financial entities in terms of size, business profiles or exposure to digital risk.*** *As a general principle, when directing resources and capabilities to the implementation of the ICT risk management framework,* ***financial entities should duly balance their ICT-related needs to their size and business profile, while competent authorities should continue to assess and review the approach of such distribution."***

DORA proposal also includes **some exemptions from certain requirements for micro enterprises** as defined in EU recommendation 2003/361 https://ec.europa.eu/growth/smes/sme-definition_en

In recital (34) of DORA proposal, it is explained that "***As larger financial entities may enjoy wider resources*** *and could swiftly deploy funds to develop governance structures and set up various corporate strategies,* ***only financial entities which are not micro enterprises in the sense of this Regulation should be required to establish more complex governance arrangements*** *(…)".*

List of exemptions for micro enterprises

According to the Commission proposal, micro enterprises are exempted from the obligations to:

1. establish a role to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services. (Article 4)
2. implement an information security management system based on recognized international standards. (Article 5)
3. ensure appropriate segregation of ICT management functions, control functions, and internal audit functions (Article 5)
4. perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their functions, supporting processes or information assets. (Article 7)
5. conduct, on regular basis, and at least yearly, a specific ICT risk assessment on all legacy ICT systems. (Article 7)

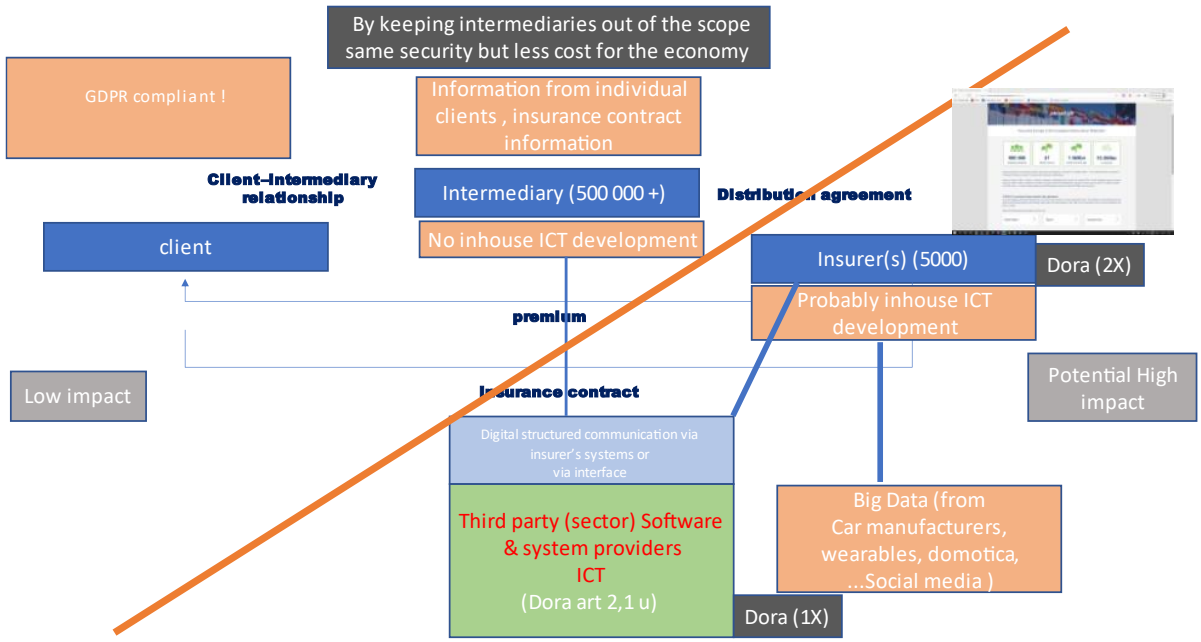
6. subject the ICT Disaster Recovery Plan to independent audit reviews. (Article 10)
7. include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities. (Article 10)
8. have a crisis management function, which, in case of activation of their ICT Business Continuity Policy or ICT Disaster Recovery Plan, shall set out clear procedures to manage internal and external crisis communications in accordance with Article 13 (Article 10)
9. report to competent authorities all costs and losses caused by ICT disruptions and ICT-related incidents (Article 10)
10. to communicate to competent authorities changes implemented to their ICT operations (Article 12)

III. BIPAR POSITION

The insurance intermediary is an intermediary… the insurance contract integrity is not influenced by the intermediary's (digital) resilience.

The impact of an IT system "shutdown" of a single intermediary (for example due to a cyber-attack) is, in macro-economic or systemic terms, inconsequential. Intermediary (over 500 000 in the EU) relationships with customers are almost exclusively treated in CRM (customer relationship management) systems. The vast majority of intermediaries (if not all) do not develop/use their own ICT system. Intermediaries use, for their clients and their policies, either the insurers' system or a market interface. Hence, they do not constitute a risk to the financial stability or to the stability in IT environments.

From a consumer/privacy perspective, any disruption is minimal (and rightly covered by the GDPR).



In practice:

- One day shutdown: there would be no consequences on the operational resilience and service continuity of the intermediary. Consumer and customer rights are safeguarded as the insurance contract information is stored by the insurer and the integrity of the contract is not affected. Other consequences are covered under GDPR, which is applicable to insurance intermediaries.

- One week shutdown: If the system of an intermediary is shut down for a week, due to a cyber-attack for example, people take over the urgent services, information can be re-assembled elsewhere (with insurers) and again, the contract integrity is safeguarded as the real commitment is the insurance contract and the insurer.

- Insurance intermediaries do not hold capital or have other connections that constitute a risk to the financial stability, or to the stability in IT environments.

- Insurance intermediaries and their activities are regulated by the Insurance Distribution Directive. Article 10.6 of the IDD in particular includes measures that protect client's money (premiums, return premiums or claims money) such as risk transfer, financial capacity requirement, segregated bank accounts and guarantee fund. In most Member States these measures have been implemented in a cumulative way.

- Insurance intermediaries are under the scope of the GDPR and therefore comply already with strict requirements regarding privacy management (risk assessment before processing data, appropriate policies and technical/organisational measures in place to prevent unlawful processing, audits to demonstrate effectiveness and compliance, security measures in place to protect personal data, data breach notification requirements).

It should be always kept in mind that DORA would impose "digital resilience" requirements on the insurers (1X compliance), while the third-party IT system (used by insures or intermediaries) will have also comply to digital resilience rules (2X compliance). In the case that DORA also imposes the same digital resilience requirements on intermediaries themselves, there will be additional compliance and security costs (3x). This results in an unnecessary economic burden.
Moreover, DORA proposal is not clear about whether compliance with digital resilience requirements can be established by using compliant third-party systems.

Furthermore, from experience in other legislations and in particular in regulations, the general proportionality principle is difficult to implement and the proposal does not provide enough information on how proportionality would be ensured.

IV. BIPAR PROPOSAL for proportionality

Based on the above, BIPAR believes that SME insurance Intermediaries should be excluded from the scope of DORA.

Reasoning:

1. **The risk factor arising from micro, small and medium intermediaries' activity does not qualify them to be financial entities subject to DORA.** The proposed DORA requirements translate to administrative burden and costs for insurance intermediaries that are not commensurate with the low risk to be addressed, nor with the general objectives to be achieved. The vast majority of intermediaries (if not all) do not develop/use their own ICT system. Intermediaries use, for their clients and their policies, either the insurers' system or a market interface. **Consequently, the communication and ICT transactions between an intermediary and an insurer are always carried out via a system in which the level of protection is guaranteed by either the insurer or the interface. By including intermediaries in the scope of DORA, the ICT-risk management requirements will be unnecessarily duplicated or triplicated.**

2. **The consequences of an intermediary not being operational for a day or a week are of extremely low risk for the insurance contract and service continuity and furthermore for the financial stability**. Macro-economically, the shutdown of an intermediary ICT system has no consequence on the provider's capability of rendering services or on the integrity of the "main-ICT system" of the insurer. Micro-economically, consumers' personal data are safeguarded as the insurance contract information is stored by the insurer and the integrity of the contract is not affected. Other consequences are covered under GDPR, which is applicable to insurance intermediaries.

3. **The Proposal's explanatory memorandum seems to confirm that costs for SME's will be significant:** "*The retained option would give rise to costs of both one-off and recurring nature. 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. The retained option would have positive effects on SMEs operating in the financial services industry in terms of economic, social and environmental impacts. The proposal will bring clarity to SMEs on what rules apply, which will reduce compliance costs*".

   This extract illustrates that the starting point were large firms. There is no detailed impact assessment or cost benefit analysis for SMEs. As currently no comparable rules are applicable to SME intermediaries (except a light regime applicable in Rumania), there is no basis to conclude that it *"will reduce compliance costs".* On the contrary, the text seems to recognise that the costs are significant; *"these costs are likely to be limited for large firms, given the significant ICT investments they have already made".*

   BIPAR would suggest studying the aspect of digital resilience in the framework of the future IDD revision so that digital resilience measures can be studied in line with the specificities of the activities and in the framework of a more specific revision of the scope of the IDD.

4. **It is challenging to ensure proportional supervision of DORA compliance in practice.** How to supervise cost -efficiently the compliance of over 500 000 intermediaries with over 100 digital checkpoints? Level playing field issues might arise.

V. EU LEGISLATIVE PROCEDURE

The EU legislators aim is to have the DORA in full effect by 2024. The proposal has been through the EU's ordinary legislative procedure, i.e. it was under examination by the European Parliament and the Council of the EU.

The EU co-legislators, the European Parliament and the Council of the EU, adopted at the end of 2021 their respective positions on the DORA Commission proposal (Digital Operational Resilience Act). They are about to officially start their negotiations (trilogue) to reach an agreement on the final text of the DORA Regulation.

Ahead of the trilogue (EP, Councul, Commission), the three positions regarding the scope and the inclusion of insurance intermediaries in DORA have been crystallized as follows:

Commission's proposal on DORA and intermediaries

Article 2 (1) (n): *DORA shall apply to "insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries".*

European Parliament on DORA and intermediaries

Article 2 (1)(n)*: DORA shall apply to "insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries that are not micro, small or medium-sized enterprises unless those micro, small or medium sized-enterprises rely exclusively on organised automated sales systems".*

The ECON Committee is in charge of the file, the EP Rapporteur is the Irish MEP Billy Kelleher (Renew Europe). The appointed shadow Rapporteurs are Irish MEP FITZGERALD Frances (EPP), German MEP KRAH Maximilian (Identity and Democracy), Maltese MEP SANT Alfred (S&D), Check MEP PEKSA Mikulas (Greens) and Polish MEP RZONCA Bogdan (ECR – Conservatives).

Council of the EU on DORA and intermediaries

Article 2 (1) (n) *DORA shall **not** apply to insurance intermediaries **which are a microenterprise or a small enterprise.***

The Council position also introduces **a new Article 14a specifying that a lighter DORA regime** will apply to **certain entities** in accordance with the proportionality principle (e.g. small and non-interconnected investment firms, payment institutions exempted under Directive (EU) 2015/2366, electronic money institutions exempted under Directive 2009/110/EC and small institutions for occupational retirement provision). Insurance intermediaries are not included in this Article 14a.

Based on the EU 2003 Recommendation:
A medium-sized enterprise is defined as an enterprise which employs fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.
A small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.
A **microenterprise** is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

Furthermore:

European Economic and Social Committee (EESC)

The EESC Opinion recommends "***raising the exemption threshold of the proposal to micro and small enterprises*** *as defined under Annex I, Article 2.2 of Commission Recommendation 2003/361/EC: enterprises which employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million and* ***reducing the number of requirements applicable to SME entities proportionally to the digital risk profile*** *of the entity could be considered*.

Joint ESAs Letter to EP, Council and Commission (February 2021)

The current DORA proposal excludes only micro-enterprises from the application of certain requirements and does not make any reference to sectoral legislation when defining the financial entities in scope.
Given this, we would like to ***suggest a more comprehensive inclusion of the principle of proportionality*** *in a more flexible way across the legal act.*