IRSG

INSURANCE AND REINSURANCE STAKEHOLDER GROUP

Advice on the Digital Operational Resilience Act

IRSG-22/14
15 April 2022

European Insurance and Occupational Pensions Authority

IRSG Position Paper on the

Digital Operational Resilience Act (D.O.R.A.)

1. General

IRSG welcomes the European Commission's Digital Operational Resilience Act (D.O.R.A.) proposal as a move in the right direction, though a move that has to be fine-tuned to a significant extent in order to achieve the desired result without bringing harmful side-effects both to consumers and the industry as a whole. It is of utmost interest to all insurance stakeholders to operate in a robust, secure and digitally mature environment since virtually all insurance companies nowadays use Information and Communication Technology. At the same time, it must be acknowledged that this overall purpose is hard to achieve without a tailored approach and with only one-size-fits-all measures1. Having that in mind, IRSG would like to express herewith some concerns that the present version of the act raises.

2. Consumer-related Issues

One major issue of concern is the cost of the envisioned transformation, as at the end of the day it will be split between the industry and the consumers. The character and proportions of this split will be decided in each and every case separately, but inevitably some part of the bill will be footed by the end-user in the form of increased price of products provided. The proposed cost estimation, accompanying the act, is rather scarce and focuses only on costs for the regulators.

The provisions focused on cases of breach and leakage of personal data should better reflect the interplay between other EU-level legislation e.g. GDPR and the respective national legislation.

3. Industry-related issues

[1] Present paper is based on the "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

The proposed act does not take into account the volume and diversity of financial sector entities, as well as of existing legacy software and hardware systems, employed by the financial/insurance industry. This, in turn, presupposes migration into new, D.O.R.A. compliant solutions without entering into the equation neither the time needed nor the resources necessary for such transformation. The proposed act switches between micro- and macro-management . It might be suggested that the should keep either high level approach to the regulated matter (recommended) or to go into details on every issue of concern. Keeping both approaches together creates a rather mixed message.

The act does not differentiate between “continuous flow” services such as e.g. payment and clearing and “batch services” e.g. insurance and pensions, applying a one-size-fits-all approach. The inclusion of a general proportionality principle, whereby entities can apply the Regulation’s provisions following a risk-based approach, would therefore be welcomed by the industry.

The proposal also mandates the ESAs to draft numerous technical standards further specifying elements of the ICT risk management framework. Given the existing level of detail of requirements in the proposal, it is important that these technical standards are not overly prescriptive to the extent that they do not leave flexibility for companies to implement them according to their own risk profile.

The use of Critical Third Party Providers (CTTP) should rely predominantly on certification since it will be practically impossible for smaller entities to make their own expert judgements about CTTP robustness. The voluntary use of certification schemes by ICT third-party service providers and financial entities should therefore be encouraged as a means of demonstrating fulfilment of and compliance with some of their rights and obligations under Chapter V of the Regulation. Such certificates can carry benefits for all parties involved. For ICT third-party service providers, certificates are a means of demonstrating adherence to quality standards and compliance with current regulations. For financial entities, making use of certificates and pooled audits can alleviate the burden on resources of performing individual audits, which might often be both unfeasible and ineffective.

The regulation does not deal sufficiently with third party dependencies - cases where software service or feature relies upon third party services or feature without written agreement.

The implementation period should be reconsidered; 1 year is overly optimistic, and the IRSG therefore calls for this period to be extended to 36 months so that insurers can properly implement the new far-reaching and comprehensive requirements.

4. Regulator-related issues

The proposal introduces a broad range of tasks for the EU-level and national level regulators. They must match the existing ability of the ESAs and the NCAs to adequately carry out their D.O.R.A. related tasks, and additional resources should be allocated to ensuring that the ESAs and competent authorities possess the technical expertise necessary to fulfil their supervisory duties under DORA. Any reliance on external expertise for the purpose of D.O.R.A. implementation should not create a potential back-door for biased final solutions.

5. In conclusion (recommendations)

IRSG reiterates its belief that D.O.R.A. is a step in the right direction but a step to be taken with many caveats, employing a higher level of technical expertise than the present case. The proposal also needs to be fine-tuned to the structure of the financial services landscape taking into duly focused consideration the proportionality issue, and flexibility must be introduced into the requirements, particularly regarding ICT risk management, so that they can be implemented by entities in a risk-proportionate manner.