OPEN LETTER OF FOUNDATION
HUMAN RIGHTS IN FINANCE.EU

To CEOs of European Institutions,
subject to Digital Operational Resilience Act (DORA)

HRIF.EU
Amsterdam
legal@hrif.eu

February 22, 2025

Re: Strategic response to DORA compliance amid geopolitical changes

Dear CEOs of EU institutions subject to the DORA-Act,

In the wake of the two-year conflict between Russia and Ukraine, the geopolitical landscape has been significantly altered, creating new challenges for financial institutions. As of last month, your companies have begun to operate under the Digital Operational Resilience Act (DORA). This new regulatory framework presents a significant challenge right from the outset.

Human Rights in Finance.EU has prepared a briefing note to guide you through the recent developments and help you assess your strategic position. Our primary request:

> **Please urgently reconsider your non-EU outsourcing policies and, at a minimum, reduce your reliance on U.S. AML rules, sanctions, and service providers**

This is not only a geopolitical imperative but also a legal requirement under DORA, which mandates that you revisit risk assessments and take appropriate action. Our attached briefing note further outlines some relevant considerations in this respect.

We understand that this fundamental shift will be a considerable challenge. Nevertheless, it is in your company's best interest to align with the DORA regulations and the upcoming Regulatory Technical Standards. Moreover, this alignment will lead to significant improvements in the protection of human rights for EU citizens and companies.

We look forward to understanding your companies' and industries' responses to the current geopolitical and market developments. We hope our briefing note will be helpful in this regard.

Thank you for your attention.

Simon Lelieveldt
Chairman - Human Rights in Finance . EU
(digital letter)

Briefing Note on the DORA-Act and Requirements for Risk Revisions – February 2025

This briefing note is prepared to assist EU companies which need to comply with the DORA-Act (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector). It focuses on the required revision of risk assessments due to current geopolitical developments.

The Legal Technicalities
DORA requires financial institutions in Europa to conduct a comprehensive risk analysis of third-party dependencies, focusing not only on technical stability but also on:

- Risk Awareness: DORA Articles 28 mandates financial entities to be aware of the risk of external providers for critical functions. Article 28 1b notes:
  - *financial entities' management of ICT third-party risk shall be implemented in light of the principle of proportionality, taking into account:*
    - *the nature, scale, complexity and importance of ICT-related dependencies,*
    - *the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities, at individual and at group level.*

- Risk Concentration: DORA Articles 29 mandates financial entities to mitigate the concentration risk and do a preliminary assessment on this. It reads:
  - *When performing the identification and assessment of risks referred to in Article 28(4), point (c), financial entities shall also take into account whether the envisaged conclusion of a contractual arrangement in relation to ICT services supporting critical or important functions would lead to any of the following:*
    - *contracting an ICT third-party service provider that is not easily substitutable; or*
    - *having in place multiple contractual arrangements in relation to the provision of ICT services supporting critical or important functions with the same ICT third-party service provider or with closely connected ICT third-party service providers.*

- Due Diligence and sanctions: The current Draft Technical Standard on ICT Service policy requires institutions to do a prior due diligence when selection service providers. It particularly mentions in article 6d the requirement to check if via the route of embargoes or sanctions the provision of critical services may be halted:
  - *is located, or processes or stores the data in a third country and, if this is the case, whether this practice affects the level of operational or reputational risks or the risk of being affected by restrictive measures, including embargos and sanctions, that may impact the ability of the ICT third-party service provider to provide the ICT services or the financial entity to receive those ICT services;*

  On the topic of sanctions, please read our separate analysis en briefing in this web-article and incorporate the Amsterdam Trade Bank case as a very likely scenario.

- Contractual arrangements: DORA Article 30(1) requires institutions to ensure proper contracting. The idea is that this should lead to regulatory compliance in storing and processing sensitive customer data, including protection against extraterritorial regulations like the CLOUD Act.
- Operational Continuity: DORA Article 11(2) mandates procedures to minimize disruptions caused by third parties and ensure contingency plans are in place and article 11 (5) clarifies that exposure to severe business disruptions needs to be done as a part of a so-called Business Impact Analysis (BIA),

Existing and future legal rules on risks/continuity for (cloud) outsourcing
With DORA in effect, some practices remain consistent while others evolve. Previously, institutions were advised (for example in DNB's Information Security Guidelines/Best Practices, p. 71) to monitor outsourcing parties for security and continuity. This approach is now formalized and expanded under DORA.

The three EU supervisors (ESAs) recently published draft technical standards specifying the content of policies related to ICT services provided by third-party service providers as mandated by Regulation (EU) 2022/2554. Notably, some banks attempted to downplay the risks associated with non-EU service providers, but the ESAs emphasized the need to consider geopolitical risks.

The New Geopolitical Reality
Recent geopolitical developments suggest a shifting international landscape, requiring financial institutions to reassess the potential risks associated with relying on service providers located in jurisdictions with differing legal and political priorities.

- On May 3, 2022: An Amsterdam Court ordered Microsoft to grant bankruptcy trustees unrestricted access to Amsterdam Trade Bank's cloud data within 48 hours,
- On January 27, 2025: The US Administration dismissed three members of the Privacy and Civil Liberties Oversight Board (PCLOB),
- On February 6, 2025: The US President signed an Executive Order imposing sanctions on ICC officials,
- On February 16, 2025: The Munich Security Conference signaled a shift to a multipolar world,
- On February 20, 2025: EU leaders convened post-Munich to push for strategic autonomy amid shifting US policies.

The DORA Oversight Framework
While DORA provides a framework for monitoring and managing third-party risks in non-EU jurisdictions, its effectiveness assumes the ex-ante cooperation of service providers and the alignment of regulatory priorities. It's not evident that this remains a corrrect assumption.

It is therefore important for EU financial institutions to consider scenarios where US-based providers may face conflicting obligations under US law, potentially impacting their ability to fully comply with EU regulations. The likelihood of the scenario of politically inspired disruption has thus significantly increased and thus mitigating measures need to change.

Risk Mitigation Alternatives
Given the significant increase in risks and likelihood of unexpected service disruptions, reliance on current legal or supervisory frameworks may no longer suffice. The ICC sanctions development demonstrate that international relations are no longer based solely on the primacy of rule of law. Therefore, the assumption must be that discontinuity of services from US-based providers could occur at any time. See also the Amsterdam Trade Bank experience.

We would suggest EU financial institutions to not wait for Overseer legal actions or mitigation of continuity problems, but take (back) control themselves. The following risk mitigation measures should now be paid attention to at the board-level of your enterprises:

- Execute exit plans and develop further alternatives for the most critical business processes with non-US based or non-US-owned providers,
- Transition other processing activities to solely EU-based operators.
- Contribute to the redesign of current EU-US structures in banking/payments/authorization/processing/storage to establish an EU-based industry consortium that is insulated from US legal leverage.
- Redesign sanctions enforcement and anti-money laundering policies, considering US dependencies and their impact.
- Update policy frameworks to disregard non-EU guidelines/FATF recommendations that conflict with EU law and the Charter of Fundamental Rights of the European Union.
- Urge the European Commission to provide legal immunity to EU companies from the extraterritorial impact of US laws.

Conclusion: it's time to redo the risks-assessments and rethink your ICT-sourcing strategy!
The financial sector is at a turning point. The continuous signals from the US government clarify that there is now a multipolar world with a new geopolitical reality.

The Digital Operational Resilience Act (DORA) provides both an opportunity and obligation to take action in the form of the obligatory revision of the risk assessment, the re-assessment of the Business Impact Assessment and the further detailing of exit-strategies and mitigating measures.

This should be done with highest urgency as the political environment is rather volatile. We can already see that the geopolitical realities shift faster than the European Commission is able to establish the Regulatory Technical Standards.

But we don't needs the finalization of those standards to know it's time to act. The strategic implications of the new world order are clear, and there is no time to waste. The race against the clock has already begun.

February 2025
Amsterdam