HOW HAWK SUPPORTS ITS CUSTOMERS TO COMPLY WITH DORA

Introduction

Since January 2025, financial institutions across the EU must comply with the Digital Operational Resilience Act (Regulation (EU) 2022/2554, "**DORA**") reshaping how such institutions manage information and communication technology ("**ICT**").

For financial institutions already navigating obligations under complex legal frameworks DORA adds a further, critical layer to ensure that the technological infrastructure of ICT third-party service providers, for example in the field of AML and transaction monitoring is resilient, secure and fully auditable.

Hawk AI GmbH ("**Hawk**") with its AI-based AML solutions supports financial institutions to comply with DORA.

Hawk as an ICT third-party service provider

Depending on the kind of implementation of Hawk's software solution, Hawk may qualify as an ICT third-party service provider under DORA.

According to Art. 3 nr. 19 DORA an ICT third-party service provider means an undertaking providing ICT services.

ICT services mean digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which include the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services (Art. 3 nr. 21 DORA).

This definition of ICT services should be understood in a broad manner to the extent that such services encompass digital and data services provided through ICT systems on an ongoing basis.[1] This includes [2]

- Software and application services (IT development; off the shelf software packages, licensing and installation thereof, etc);
- Network infrastructure services (excluding telecommunication services);
- Data centers (physical data centers space and basic utilities);
- ICT consultancy and managed ICT services;
- Information security and cybersecurity services (including control and monitoring, penetration testing, security operations centers, etc.);
- Cloud computing (covering all service models and types) and
- Data analysis and other data services (provision of data, data entry, data storage, data processing and reporting services, data monitoring as well as data-based business and decision support services).

Hawk provides a Software-as-a-Service (SaaS) solution and develops AI-based software products for regulated financial institutions to analyse and monitor financial transactions with the aim of detecting illegal activities such as money laundering or fraud at an early stage ("**Solutions**") for financial entities to meet their AML obligation (e.g. Sec. 10(1) Nr. 5 German Money Laundering Act).

According to a Q&A published by the EU Commission services that are "ancillary" to financial services provided in a standalone manner and unrelated to, or independent from, regulated financial services, are considered ICT services.[3]

The Hawk Solutions are designed as ancillary services in respect of AML obligations of regulated customers provided independent of financial services of such customers. The Solutions include in particular:

- Real-time transaction monitoring
- Pattern recognition in payment data (machine learning)
- Screening of financial institutions' customers against PEP and sanctions lists
- Automated alert generation for the escalation of suspicious cases;
- Support for compliance officers in financial institutions.

Typically, the Solutions are embedded in customers' AML systems and therefore constitute ICT services, meaning that Hawks itself qualifies as an ICT third-party service provider.

The Solutions are technically based on supervised learning models, which use customer's historical data and feedback from false positive classifications for optimization. The system does not take autonomous decisions with final character such as refusal of transactions, or submission of a suspicious activity report to a supervising authority but merely provides the customers' compliance staff with a structured basis and risk-score (both anomaly as well as false positive reduction score) for decision-making.

How Hawk supports DORA compliance

DORA requires financial institutions not only to manage their own ICT risks but also risks relating to ICT third-party service providers that supply them.

According to Art. 3 nr. 18 DORA ICT third-party risk means an ICT risk that may arise for a financial institution in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements.

When a regulated financial institution outsources certain services or obligations, it must negotiate key contractual provisions with the outsourcing service provider including with regard to (i) the integrity and security of data, (ii) incident reporting processes, (iii) audit rights and (iv) exit or termination strategies. Financial institutions cannot contract with ICT third-party service providers who do not meet these requirements. Competent authorities will have the authority to suspend or terminate contracts that do not comply with DORA's third-party risk requirements.

Financial institutions must also assess their third-party ICT dependency risk and monitor the performance of such providers.

These obligations respond to the increasing operational reliance on external technology providers especially in areas such as transaction monitoring, fraud detection and customer due diligence.

Hawk's Solutions enable financial institutions to meet these requirements outlined by DORA regarding their ICT third-party service providers. Hawk has structured its Solutions, documentation and contractual frameworks to help its customers to meet these requirements. In the following we illustrate Hawk's capabilities based on the following examples:

ICT third-party service providers/subcontractors used by Hawk

As mentioned, Hawk's customers as financial institutions regulated under DORA need to manage ICT third-party service providers' or ICT subcontractors' risks.

Therefore, such customers are required to:

- Know Hawk's ICT service supply chain, meaning comprehending ICT third-party service providers or subcontractors used by Hawk (Art. 28 DORA);
- A concentration and substitution risks of such providers or subcontractors (Art. 29 DORA) and
- Ensure such providers or subcontractors are appropriately managed and contractually bound (Art. 30 DORA).

Main dependencies of Hawk's services to third parties are the cloud services required to offer Hawk's Solutions.

Cloud services provided by a third party and used by Hawk to provide its services qualify as ICT services. In particular, cloud infrastructure, platform services, platform hosting and data storage for Hawk are provided by such third party. Those services are essential ICT services to Hawk with indirect access to processing environments, implying operational reliance used for core parts of its customer offering.

Hawk provides all information needed for such (sub-)provider of ICT cloud services to its customers to facilitate ICT risk management assessments of Hawk and its ICT subcontractors.

Contractual Arrangements (Art. 30 DORA)

According to Art. 30 DORA financial institutions need to ensure the mandatory rights and obligations under DORA are contractually allocated with their ICT third-party service providers.

Hawk fulfils these requirements via its main service agreement, which includes a DORA specific addendum and Data Processing Agreement. Hawk contractually commits to:

- Data processing and residency provisions on data location and protection (Art. 30(2)(a) DORA);
- The availability, authenticity, integrity and confidentiality of the data processed as part of the ICT service, in particular personal data (Article 30(2)(c) DORA);
- Incident reporting obligations, which ensure that relevant ICT-related disruptions or security events are promptly communicated (Article 30(2)(g) DORA);

- Access, inspection and audit rights for the customer and if applicable, competent authorities (Article 30(2)(h) DORA);

- Termination and exit clauses including data portability mechanisms and transition support, allowing continuity of critical functions if the contractual relationship is discontinued (Article 30(2)(j) DORA).

Risk Assessment and Performance Monitoring

Before entering into any ICT outsourcing agreement, financial institutions must conduct a prior risk assessment that evaluates the ICT third-party service provider's operational reliability and the potential concentration or substitution risk (see Art. 28 f. DORA).

Hawk provides its customers with extensive due diligence materials to conduct such risk assessment, including:

- **ISO 27001 certification**

  Both ISO 27001 and DORA place a significant emphasis on establishing and maintaining a risk management framework. Hawk's ISO 27001 certification provides a strong foundation for compliance with DORA's risk management requirements and control systems. ISO 27001 allows Hawk to determine gaps and reaching DORA compliance. In addition, ISO 27001 allows to evidence compliance with new regulations in an easy manner. ISO 27001 certification does increase the likelihood of auditors and regulatory authorities' approval of Hawk organisation's digital resilience.

- **Penetration testing results**

  Generally, HAWK conducts its own threat-led penetration testing.

- **Internal policies**

  Governing incident management, data handling, model governance and business continuity.

- **SLA monitoring and uptime/performance reports**

  Hawk regularly provides service level updates.

Exit Strategies and Business Continuity Provisions (Art. 28 DORA)

Art. 28 DORA requires financial institutions to ensure that any disruption of (ICT) services does not disrupt their operations or prevent the continued performance of critical functions.

Hawk addresses this requirement with an exit and transition planning framework. Such framework includes:

- Customers maintaining full ownership of their data, including transaction logs, audit trails, case decisions and model configurations;

- Escrow and

- Exit support re-offboarding.

Conclusion

DORA introduces comprehensive requirements for financial institutions to manage third-party ICT risks. Due to these requirements financial institutions need to treat ICT third-party service providers with a high level of scrutiny, accountability and resilience.

Hawk has structured its customers' contractual relationships, AML solutions and governance documentation accordingly to help its customers comply with DORA.