FINANCIAL SERVICES INDUSTRY ADDENDUM (DORA)

[Last Updated: February 7, 2026]

This Digital Operational Resilience Act Addendum ("**DORA Addendum**" or "**Addendum**") is applicable solely to Customers from the Financial Service Industry ("**FSI**") established in the EEA and are subject to the Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector ("**DORA**"). This DORA Addendum is meant to meet DORA requirements and obligations.

To the extent applicable, this DORA Addendum is part of the Master Service Agreement ("**MSA**") or End User Licensing Agreement ("**EULA**"), as applicable (each, the "**Agreement**"), governing the use of the information and communication technology services procured by Customer under the Agreement ("**ICT Services**"). In the event of any conflict or inconsistency between this DORA Addendum and the Agreement, this DORA Addendum will prevail solely to the extent necessary to comply with DORA, otherwise the Agreement will prevail.

1. DEFINITIONS

Capitalized terms used but not defined in this Addendum will have the same meanings as either defined under DORA, or as provided in the Agreement that includes, as applicable, the SLA, Information Security Policy, and Data Protection Addendum ("**DPA**"). The following definitions are used in this Addendum:

1.1. "**Financial Services**" means, without limitation, banking, credit, insurance, payment services, stock brokering, futures trading, stock exchanges, issuing electronic money, and other services involving the investment, lending, trading, and management of money and assets.

1.2. "**ICT-related Incident**" means a single event or a series of linked events unplanned by the Customer that compromises the security of the network and information systems and has an adverse impact on the availability, authenticity, integrity, or confidentiality of data, or on the services provided by Customer.

1.3. "**Regulator(s)**" means any competent authority, resolution authority, or other regulatory body with binding authority to regulate, supervise, or govern Customer activities, or Akeyless' as the provider of the ICT Services.

1.4. "**Service Levels**" means the service levels detailed in the SLA.

1.5. "**Sub-processor**" or "**Subcontractor**" shall refer to the vendors listed in the Sub-processor list: https://www.akeyless.io/list-of-sub-processors/

2. SCOPE OF ICT SERVICES

2.1. **Description of Services**: Akeyless provides cloud-based SaaS solution, multi-cloud secrets management platform, enabling enterprises and organizations to secure and manage authorizations, access, and permissions to IT and Cloud environments, all as detailed herein: https://docs.akeyless.io/ and https://docs.akeyless.io/docs/akeyless-overview

2.2. **Designation of Critical or Important Functions**: Customer shall notify Akeyless in writing if it determined that the ICT Services constitute ICT services supporting critical or important functions for the purposes of Article 30(3) of DORA. Absent such written notification from Customer, the ICT Services shall be deemed non-critical services, and the provisions of this Addendum applicable only to critical or important functions shall not apply.

2.3. **Responsibility**: Customer acknowledges and agrees that the final responsibility for DORA compliance remains with Customer. Provider's obligations under this Addendum are supplementary to, and do not substitute for, Customer's own obligations under DORA.

2.4. **Service Locations**: the locations where the ICT Services are provided, including where Customer Data is processed or stored, are specified in the Sub-processor list: https://www.akeyless.io/list-of-sub-processors/. Akeyless will provide prior written notice, through the account or via email correspondence, if Akeyless materially changing such service locations.

3. SUBCONTRACTING

3.1. Customer acknowledges and agrees that Akeyless may subcontract the performance of all or any part of its obligations under the Agreement (including the provision of the ICT Services) to affiliates, Sub-processors or third-party subcontractors ("**Subcontractors**"), subject to the following conditions:

3.1.1. Prior to engaging with third-party contractors and subcontractors (including Sub-processors), Akeyless performs a reasonable due diligence check, including on such Subcontractors' security standards, to ensure compliance with Akeyless' standards for data security protection. This may include a review of risk assessments, audits, and physical, technical, organizational, and administrative controls.

3.1.2. Akeyless reviews its Sub-processors on an annual basis.

3.1.3. The Subcontractor agreements, will include, where possible, audit rights, at least in the event of a security incident, conducted either by Akeyless, its customer, or Regulator.

3.2. Akeyless shall remain fully responsible for the acts and omissions of its Subcontractors.

3.3. A list of Subcontractors is available at all times here: https://www.akeyless.io/list-of-sub-processors/. Subject to Customer registering for notifications, Akeyless shall notify Customer of material changes to subcontracting arrangements affecting Customer Data. If Customer establishes that such material changes expose Customer to unreasonable risk, Customer may object to such changes in writing within thirty (30) days of the notification. In the absence of an objection within such period, Customer is deemed to have accepted such change.

3.4. Customer agrees that Akeyless is not obligated to provide Customer with veto rights over subcontracting decisions, except to the extent specifically set forth herein or expressly required by DORA.

4. SECURITY AND CUSTOMER DATA

4.1. Akeyless shall implement and maintain appropriate technical and organizational measures designed to ensure the availability, authenticity, integrity, and confidentiality of Customer Data as detailed, and updated from time to time here: https://www.akeyless.io/data-protection-measures/ and in the Akeyless Trust Center.

4.2. Personal Data shall be processed subject to the DPA: https://www.akeyless.io/data-processing-agreement/.

4.3. During the Term, Customer shall be entitled to access and retrieve Customer Data. In the event of insolvency, resolution, or discontinuation of Akeyless' business operations, or in the event of termination of the Agreement or ICT Services, Akeyless shall ensure access, recovery, and return in an easily accessible format of Customer Data for a period of thirty (30) days following termination ("**Transition Period**") or such event, unless Customer has selected a shorter data retention period.

4.4. Akeyless maintains comprehensive ICT security awareness programs and digital operational resilience training for its personnel involved in the provision of ICT Services. Akeyless places a strong emphasis on security awareness and training for all employees, recognizing the importance of understanding their information security responsibilities. A mandatory annual security awareness training program is in place for all employees. This training covers critical areas such as common security risks and threats, compliance with regulations, data protection and customer privacy, security, and awareness of social engineering tactics including fraud and phishing.

4.5. Following the above, Akeyless shall not be required to participate in Customer's internal training or awareness program if Akeyless provides information reasonably necessary to demonstrate that Akeyless' internal program sufficiently addresses the security awareness objectives relevant to the ICT Services provided. To the extent Akeyless is unable to demonstrate such alignment, Akeyless may participate in Customer's training initiatives. Customer training shall be provided free of charge.

5. ICT INCIDENT MANAGEMENT

5.1. Akeyless shall notify the Customer in the event of an ICT-related Incident that materially impacts ICT Services, without undue delay upon confirmation of the incident, together with reasonable details of the incident and any steps being taken to mitigate its effects.

5.2. Akeyless shall provide reasonable assistance to Customer in the event of an ICT-related Incident that is directly related to the ICT Services and that arises as a result of Akeyless act or omission.

5.3. An ICT-related Incident that results in whole or in part from Customer's failure to maintain appropriate security arrangements, Customer's failure to meet any minimum system requirements notified by Akeyless, or Customer's use of the ICT Services other than in accordance with the Agreement, Documentation or instructions, shall not be deemed attributable to Akeyless, and Akeyless may provide support and assistance with respect to such incidents at its sole discretion.

6. **REGULATOR AND CUSTOMER AUDIT AND MONITORING RIGHTS**

6.1. Akeyless shall reasonably cooperate with Regulators and any representative appointed by them in matters related to Akeyless' obligations under this DORA Addendum, to the extent required by Applicable Laws and subject to the confidentiality provisions in the Agreement.

6.2. In the event a Regulator initiates an information request from Akeyless regarding ICT Services provided to Customer, Akeyless shall fully cooperate as it relates to access to such information for the purposes of determining compliance with DORA, provided that Customer provides Akeyless with reasonable prior written notice of such requests to the extent permitted by law.

6.3. Customer acknowledges and agrees that, due to the rights of Akeyless' customers, Akeyless cannot provide Customer or any Regulator with unrestricted rights of access, inspection, and audit or the right to take copies of documents as contemplated by Article 30(3)(e) of DORA. Accordingly, pursuant to Article 30(3)(e)(ii) of DORA, the Parties agree to the following alternative assurance measures:

6.3.1. **Third-Party Certifications and Audit Reports:** Subject to confidentiality obligations, Akeyless agrees, upon Customer's written request (and no more than once per calendar year), to provide copies of relevant third-party certifications, including ISO 27001, SOC 2 Type II, and other applicable compliance certifications maintained by Akeyless, or provide copies of third-party or internal audit reports covering the systems and key controls relating to the ICT Services.

6.3.2. **Compliance Questionnaires:** Akeyless shall provide written responses, on a confidential basis, to reasonable requests for information made by Customer, including responses to information security and audit questionnaires, in each case which are reasonably required to confirm Akeyless' compliance with the Agreement.

6.3.3. Customer agrees to rely on third-party certifications, third-party or internal audit reports, and compliance questionnaires made available by Akeyless to the extent permitted under DORA. Only in the case where all such information and documentation provided by Provider does not evidence that Provider complies with its contractual obligations under this DORA Addendum shall Customer request an onsite inspection or audit.

6.4. If Customer, notwithstanding the foregoing, requires an on-site audit to comply with DORA requirements or a Regulator binding request, such audit shall be subject to the following conditions:

6.4.1. Customer shall submit a detailed audit plan at least ninety (90) days in advance of the proposed audit date to Akeyless, describing the scope, duration, and start date of the audit. Akeyless will review the audit plan and provide Customer with any concerns or questions ensuring Akeyless' (including its digital asset, platform, Services and customers) security, privacy, employment, or other relevant rights.

6.4.2. The audit shall be limited to once per year, unless otherwise required by law.

6.4.3. If the requested audit scope is addressed in a similar audit report or certification within the prior twelve (12) months and Akeyless confirms there are no material

changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

6.4.4. The audit must be conducted during regular business hours at the applicable facility and may not interfere with Akeyless' business activities or with Akeyless' confidentiality obligations to other customers. Where other customers rights may be affected, Akeyless may require alternative assurance levels, including pooled audits.

6.4.5. The auditor conducting the audit on Customer's behalf must not be Akeyless' competitor or associated with a competitor, and such third-party is subject to Akeyless' prior written approval. The auditor must execute a written confidentiality agreement before conducting the audit. Customer may use the audit reports only for the purpose of meeting the regulatory requirement that gave rise to the audit. The audit reports and any other materials, documents, communications or information relating to the audit are Akeyless' Confidential Information.

6.4.6. Customer will provide Akeyless with a copy of any audit reports generated in connection with any audit, unless prohibited by applicable Laws.

6.5. All audits are at Customer's sole expense. Any request for Akeyless to provide assistance with an audit is considered a separate service, and Akeyless reserves the right to charge Customer with additional fees.

7. RESILIENCE TESTING, BCP AND DISASTER RECOVERY PLAN

7.1. Akeyless confirms that it regularly tests its resilience measures, including penetration testing, vulnerability assessments, and other controls, in accordance with industry standards and best practices.

7.2. Akeyless maintains and regularly tests business contingency plans ("**BCP**") to ensure a continuous as further detailed in the Information Security Policy available at https://www.akeyless.io/data-protection-measures/.

7.3. As the Threat-Led Penetration Testing ("**TLPT**") may have an adverse impact on the quality or security of the services that Akeyless provides to its other customers, Akeyless reserves the right to engage an external tester to perform pooled testing in accordance with DORA Article 26(4), rather than participate in Customer-led individual TLPT.

7.4. Akeyless also implements robust vulnerability management, conducting regular internal scans and quarterly production network scans, ensuring timely remediation of high-risk vulnerabilities, including in source code as part of the SDLC. High or Critical issues are investigated and dealt with in accordance with Akeyless SDLC process or by any necessary means. Following that, a re-test is performed to verify the remediation of the relevant issues.

7.5. Quarterly external network scans of the Services are conducted and monthly vulnerability test are conducted. Response time for known vulnerabilities that are **critical** [As soon as possible and no longer than 1 week from identification], **high** [No longer than 1 month from identification] **medium** [No longer than 3 months from identification] **low** [No longer than 3 months from identification].

7.6. Akeyless maintains backup policies and associated measures. Such backup policies include the constant monitoring of operational parameters, as relevant to the backup operations. Furthermore, the servers include an automated backup procedure. Akeyless will create and maintain disaster recovery plans to restore customer-facing cloud products to customers. Disaster recovery plans will define Recovery Time Objectives ("**RTO**") and Recovery Point Objectives ("**RPO**") for the Services.

- RTO of the Customer Data: 1 hour
- RPO of the Customer Data: 1 hour

8. TERMINATION RIGHTS, EXIT PLANS

8.1. In addition to the termination provisions in the Agreement, Customer may terminate the Agreement by providing at least 30-day prior written notice if (i) a Regulator has required termination; (ii) material change to the ICT Services that no longer comply with laws applicable to Customer as a regulated FSI; (iii) Customer demonstrated that there are weaknesses regarding the management and security of Customer Data or information which

was not cured within 30-days from providing Akeyless with such notice; or (iv) Subcontractor replacement despite Customer's objection to such Subcontractor.

8.2. Prior to exercising any termination right Customer shall provide Akeyless with documented evidence supporting the basis for termination (such as a copy of an internal risk assessment or communication from a Regulator)

8.3. Customer shall pay Akeyless all fees and charges payable in respect of the provision of the ICT Services for the period up to and including the date of termination, including any outstanding fees on orders committed. Termination of the ICT Services under this Section shall not entitle Customer to any refund of prepaid fees, and Customer shall remain liable for all fees otherwise due under the Order Form or Agreement, as applicable.

8.4. Customer acknowledges and agrees that, given the nature of ICT Services, it is unlikely that extensive transition or exit assistance services will be required upon the termination or expiry of the Agreement.

8.5. In the event that Customer requires transition or exit assistance services upon the termination or expiry of the Agreement, Akeyless agrees to provide such services, provided that the scope, duration, and nature of the services is commercially reasonable and is agreed in writing between the parties and Customer pays for such services, in addition to the then current Subscription fees. Customer is responsible for developing its own plan for the orderly transition and exit from the ICT Services by leveraging available capabilities and features of ICT Services.

9. MISCELLANEOUS

9.1. **Severability.** Should any provision of this DORA Addendum be held or declared invalid, unlawful, or unenforceable by a competent authority or court, then the remainder of this DORA Addendum shall remain valid.

9.2. **Notice.** Instructions, notices, and other communications made under this DORA Addendum shall be made in accordance with the notice provisions of the Agreement.

9.3. **Amendments.** Akeyless may update this DORA Addendum from time to time by publishing an updated version (including by posting it to Akeyless' website or through Customer's Account) Unless otherwise stated by Akeyless, any updates will become effective ten (10) days after publication. Notwithstanding the foregoing, if Akeyless makes a material revision to this DORA Addendum, Akeyless will provide Customer with notice (including via email or through Customer's Account), and such revision will become effective thirty (30) days after such notice.

9.4. **Term.** This DORA Addendum shall remain effective as long as there is an effective Order Form and Agreement, and to the extent Customer is subject to DORA or defined a Financial Entity, and shall automatically terminate upon the earlier of: (i) the expiry or termination of the Agreement or Order Form; or (ii) the date on which Customer is no longer subject to DORA. However, the remaining provisions of this Addendum shall continue in full force and effect unless otherwise agreed by the Parties

9.5. **Fees.** Unless specifically agreed otherwise in writing, Akeyless shall be entitled to charge reasonable fees for activities undertaken in the fulfillment of its obligations under this DORA Addendum that are in addition to the services already contracted under the Agreement.

9.6. This Addendum is governed by the law and jurisdiction provisions of the Agreement, except to the extent otherwise mandated by applicable laws and regulations administered by the regulatory body in the European Union, with binding authority to regulate, supervise or govern Customer's financial services activities under DORA, including the resolution authorities of regulated entities.