DORA Explanatory Note and Provisions Mapping

The Digital Operational Resilience Act ("**DORA**"), is a European Union regulation that aims at maintaining a high level of digital operational resilience for the **financial sector**. DORA seeks to enable a strong and effective ICT risk management by financial entities. In that regard, DORA establishes mandatory rules, including requirements for a thorough pre-contracting analysis of vendor ICT risk. This includes, among other things, the renegotiation of contractual agreements between financial entities and vendors and the application of due diligence by financial entities in the process of the selection and assessment of vendors.

Pursuant to Article 2(e) of DORA, Akeyless is defined an ***'ICT third-party service provider'*** and the customer is the financial entity. Therefore, DORA will apply to Akeyless indirectly, in case a Customer falls to the ***"financial entity"*** definition under DORA and defines Akeyless as one of its ICT providers.

DORA mandates that financial entity (i.e., the Akeyless Customer) shall ensure that certain **contractual terms** are embedded in the relevant contractual agreements between the parties. DORA requires that the mandatory terms are incorporated **prior to 17 January 2025**. For this purpose, Akeyless has taken a proactive approach and has updated all legal documentation to include the needed provisions according to DORA, all as detailed below.

Further, DORA mandates that the financial entity shall apply due diligence in the selection and assessment of its vendors, both prior to onboarding a vendor, or in case of a current existing vendor, the DORA madidates on going assessment and yearly reviews. Akeyless is happy to respond to any needed questionnaires and participate in such assessments, for more information on Akeyless' security practices please see here:

- https://www.akeyless.io/data-protection-measures/
- https://www.akeyless.io/trust-center/

The DORA mandates that financial entities shall discontinue/terminate the relevant agreements with vendors, who do not consent to the incorporation of the mandatory terms, or who do not cooperate for the successful completion of the due diligence assessment.

To comply with these obligations, we understand that our customer rely on Akeyless' cooperation and Akeyless has independently updated the Master Services Agreement (MSA), the End User License Agreement (EULA) (https://www.akeyless.io/end-user-license-agreement/), the Service Level Agreement (SLA) (https://www.akeyless.io/service-level-agreement/), the Information Security Policy (https://www.akeyless.io/data-protection-measures/), the Subcontractor list (https://www.akeyless.io/list-of-sub-processors/) and the Data Processing Agreement (https://www.akeyless.io/data-processing-agreement/), all to ensure the needed provisions under DORA are met.

PROVISIONS MAPPING

APPLICABLE PROVISIONS	DORA ARTICLE
Section 15.3 and Section 15.5 of the Information Security Policy	30 (2) a DORA

Section 2.1 of the EULA and Section 2.1 in the MSA provide the description of the services as required under DORA.	30 (2) a DORA
Section 2.2 in the EULA and in the MSA provide the (full) service level descriptions (including the SLA).	30 (2) e DORA + 30 (3) a DORA
Data Protection matters are governed by the Data Processing Agreement as well as Section 10 of the MSA and EULA, as applicable.	30 (2) c DORA
The locations of processing are stipulated in various section in the MSA and EULA, in the Information Security Policy and in the Subcontractor page.	30 (3) b DORA
See SLA and Section 2.2 of the MSA and EULA, as applicable.	30 (3) a DORA
Section 13 of the Information Security Policy, and Section 9 of the MSA or EULA as applicable.	30 (3) c DORA
Section 13 of the Information Security Policy, and Section 9.4 of the MSA or EULA as applicable.	30 (3) c DORA
Information Security Policy	28 (5) + 30 (2) c DORA + 30 (3) (c)
Section 14 of the Information Security Policy	30 (2) c DORA + 30 (3) (c)
Section 10.4 of the EULA and MSA, as applicable, set Customer's right to retrieve and access Customer Data.	30 (2) d DORA
Section 12 of the Information Security Policy and Section 9.3 of the MSA or EULA as applicable.	30 (2) f DORA
Section 7.6 of the MSA or EULA set out the right to retrieve Customer Data	30 (3) d DORA
Audit provisions available in the Information Security Policy, including section 15.4 in the MSA and 15.5 in the EULA.	30 (2) g DORA
Section 16 of the Information Security Policy	30 (3) e (i-iii) DORA
Section 16 of the Information Security Policy	30 (3) e (i) + (iv) DORA
Section 7.6 of the EULA or MSA as applicable set out the transition period.	30(3)(f) DORA
Section 7.2 and 7.3 of the MSA and EULA provide immediate termination for regulatory breach as required under DORA.	28 (7) a DORA + 30 (2) h DORA
Section 16.2 of the Information Security Policy and Section 7.3 of the MSA or EULA, as appliable.	28 (7) b DORA
Section 7.3 of the MSA and EULA as applicable.	28 (7) d DORA
The service levels are detailed in the SLA.	30 (2) e DORA