Data Privacy Framework Statement

Akeyless Security USA Inc. ("**Akeyless**") is self-certified for compliance with the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**") and the UK Extension to the EU-U.S. DPF ("**UK Extension to the EU-U.S. DPF**") (collectively – "**DPF Principles**"), as set forth by the U.S. Department of Commerce.

If there is any conflict between the terms in this Data Privacy Framework Statement and the DPF Principles, the DPF Principles shall govern. To learn more about the DPF Principles please visit https://www.dataprivacyframework.gov/. To view our certification, please visit https://www.dataprivacyframework.gov/list.

Akeyless Security Ltd. provides a cloud-native SaaS platform for "zero trust" data encryption technology specializing in unified secrets and machine identity management to its customers. Akeyless is a fully owned subsidiary of Akeyless Security Ltd. (collectively "**Akeyless Group**"), providing certain services to Akeyless Security Ltd. These services include, among others, marketing, sales and customer success management services. Akeyless processes personal data solely for the purpose of providing its SaaS cloud-based solution. The personal data processed are contact information, access logs, and potentially the meta-data encrypted, among others.

Our Privacy Policy available at: https://www.akeyless.io/privacy-policy/ outlines the purposes and uses of personal data. If Akeyless intends to process personal data for a purpose that differs significantly from the original purpose(s) for which it was collected, we will seek your consent and will not proceed without obtaining it.

Onward Transfers of Personal Data. For onward transfers of personal data to third parties, Akeyless is responsible for ensuring that these third parties adhere to applicable data protection principles, including ensuring that the third parties do not process such personal data in a manner inconsistent with the DPF Principles.

Independent Recourse Mechanism and Arbitration. In line with the DPF Principles, Akeyless is committed to addressing all EU-U.S. DPF-related complaints regarding our collection and use of your personal data in accordance with the DPF Principles. EU and UK individuals with inquiries or complaints regarding our handling of personal data under the DPF Principles should first reach out to us at: privacy@akeyless.io. We will investigate and strive to resolve any complaints or disputes related to the Data Privacy Framework within forty-five (45) days of receipt.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Akeyless commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of personal data received in reliance on the DPF Principles.

Please note that if your complaint is not resolved through these methods above, a binding arbitration option may be available under limited circumstances. Additional information can be found here: https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction.

U.S. Federal Trade Commission Enforcement. Additionally, Akeyless is subject to the investigatory and enforcement powers of the Federal Trade Commission ("**FTC**"), which oversees Akeyless's compliance with the DPF Principles. Under certain conditions, individuals may have the option to initiate binding arbitration for unresolved complaints concerning DPF compliance that

other DPF mechanisms have not addressed. For further details, please see Annex I of the DPF Principles.

Notwithstanding the above, under certain circumstances, Akeyless may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.