DATA PROCESSING AGREEMENT

Last Updated March 18, 2026

This Data Processing Agreement ("**DPA**") is governed by and hereby attached to the Master Service Agreement, Terms of Service, or any other agreement ("**Agreement**") executed by and between Akeyless Security Ltd. or Akeyless Security USA Inc. ("**Akeyless"**), and you, a customer, user or individual ("**Customer**"). Akeyless and Customer shall each be referred to as "**party**" and collectively as "**parties**".

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

WHEREAS, Akeyless is the developer and operator of a cloud-based SaaS solution enabling enterprises and organizations to secure and manage authorizations, access, and permissions to IT and Cloud environments ("**Akeyless Technology**"), all as agreed by the parties in the applicable order form or other ordering documents that are incorporated in the Agreement (collectively the "**Service(s)**"); and

WHEREAS, the Services may require Akeyless to Process Personal Data (as such terms are defined below) on Customer's behalf, which Customer discloses to Akeyless only for the limited and specified purposes set forth herein, and subject to the terms and conditions of this DPA.

THEREFORE, the parties desire to achieve compliance with the UK, EU, Swiss, United States, Israeli and other data protection laws and agree on the following:

1. DEFINITIONS

1.1. "**Adequate Country**" is a country that received an adequacy decision from the European Commission or other applicable data protection authority.

1.2. The terms "**Business**", "**Business Purpose**", **"Consumer",** "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" (and "**Process**"), "**Processor**", "**Holder**", **"Sensitive Data", "Service Provider", "Sale" (or "Sell") and "Share",** "**Special Categories of Personal Data**" and "**Supervisory Authority**", shall all have the same meanings as ascribed to them under applicable Data Protection Laws. Further, under this DPA "**Data Subject**" shall also mean and refer to a "**Consumer**", and "**Personal Data**" shall also mean and refer to "**Personal Information**", and "**Special Categories of Data**" or "**Highly Sensitive Data**" shall also mean and refer to "**Sensitive Data**".

1.3. "**Customer Data**" means Customer Data (as defined in the Agreement) containing Personal Data processed by Akeyless in the course of its Services provision to Customer, all as detailed in **Annex I** attached herein.

1.4. "**Data Privacy Framework**" or "**DPF**" means the EU-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework operated by the U.S. Department of Commerce, operated by the U.S. Department of Commerce; as may be amended, superseded or replaced.

1.5. "**Data Privacy Framework Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework available at:

https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles; as may be amended, superseded or replaced.

1.6. "**Data Protection Law**" means any and all applicable privacy and data protection laws and regulations, including, where applicable, EU Data Protection Law, UK Data Protection Laws, Swiss Data Protection Laws, Israeli Data Protection Laws and the US Data Protection Laws, as may be amended or superseded from time to time, and any judicial or administrative interpretation of such laws, including any binding guidance, guidelines, codes of practice, approved codes of conduct or certification mechanisms approved by the applicable authority.

1.7. "**EEA**" means the European Economic Area.

1.8. "**European Data Protection Laws**" means collectively, the laws and regulations of the European Union, the EEA, their member states, and the United Kingdom, applicable to the Processing of Personal Data, including (where applicable): (i) EU General Data Protection Regulation (Regulation 2016/679) ("**EU GDPR**"); Regulation 2018/1725; and the e-Privacy Directive (Directive 2002/58/EC), as amended (**e-Privacy Law**); (ii) "**UK Data Protection Laws**" - the Data Protection Act 2018 (DPA 2018), as amended, and EU GDPR as incorporated into UK law as amended ("**UK GDPR**" and collectively with the EU GDPR shall be referred to herein as the "**GDPR**"); (iii) "**Swiss Data Protection Laws**" or "**FADP**" - the Swiss Federal Data Protection Act (dated June 19, 1992, as of March 1, 2019) ("**FDPA**") and the Ordinance on the Federal Act on Data Protection ("**FODP**"); (iv) any national data protection laws made under, pursuant to, replacing or succeeding the EU GDPR or the e-Privacy Law; (v) any amendment or legislation replacing or updating any of the foregoing; and (vi) any judicial or administrative interpretation of any of the above, including any binding judicial or administrative interpretation of any of the above, or approved certification mechanisms issued by any relevant Supervisory Authority.

1.9. "**Instructions**" means the written, documented instructions issued by the Customer to Akeyless directing Akeyless to perform a specific or general action with regard to Customer Data (including, but not limited to, instructions to provide the Services under the Agreement and instructions under this DPA).

1.10. "**Israeli Data Protection Laws**" means, collectedly, the: (i) Israeli Privacy Protection Law, 5741-1981; (ii) the regulations promulgated pursuant thereto, including the Israeli Privacy Protection Regulations (Data Security), 5777-2017 and the Israeli Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001; (iii) any amendments or legislation replacing or updating any of the foregoing, and; (iv) any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or certification mechanisms approved by the Israeli Privacy Protection Authority .

1.11. "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data. Any Personal Data Breach will comprise a Security Incident.

1.12. "**Standard Contractual Clauses**" or "**SCCs**" means (i) the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission Decision 2021/914 of 4 June 2021, which may be found here

(ii) the UK "International Data Transfer Addendum to the European Commission Standard Contractual Clauses" available at: https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf and incorporated herein by reference ("**UK SCC**"); or (iii) the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner ("**Swiss SCC"**).

1.13. "**US Data Protection Laws**" means any U.S. federal and state privacy laws and regulations effective as of the Effective Date of this DPA and applies to Akeyless Processing of Customer Data, and any implementing regulations and amendment thereto, including without limitation, the (i) California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 – 1798.199) of 2018 including as modified by the California Privacy Rights Act as well as all regulations promulgated thereunder from time to time ("**CCPA**"), (ii) the Colorado Privacy Act C.R.S.A. § 6-1-1301 et seq (SB 21-190) ("**CPA**"), the (iii) the Connecticut Data Privacy Act, S.B. 6 (Connecticut 2022) ("**CTDPA"**); (iv) Delaware Personal Data Privacy Protection Act ("**DPDPA**"); (v) the Florida Digital Bill of Rights S.B 262 ("**FDBR"**); (vi) the Indiana Consumer Data Protection Act ("**ICDPA**"); (vii) the Iowa Consumer Data Protection Act ("**ICDPA**"); (viii) the Kentucky Consumer Data Protection Act ("**KCDPA**"); (ix) the Maryland Online Consumer Privacy Act ("**MOCPA**"); (x) the Minnesota Consumer Data Privacy Act ("**MCDPA**") (xi) the Montana Consumer Data Privacy Act 68th Legislature 2023, S.B. 0384 ("**MTCDPA"**); (xii) the Nebraska Data Privacy Act ("**NDPA**"); (xiii) the New Hampshire Data Privacy Protection Act ("**NHDPA**"); (xiv) the New Jersey Data Protection Act ("**NJDPA**"); (xv) the Oregon Consumer Data Privacy Act ORS 646A.570-646A.589 ("**OCDPA"**); (xvi) the Rhode Island Data Transparency and Privacy Protection Act ("RIDTPPA"); (xvii) the Texas Data Privacy and Security Act, Tex. Bus. & Com. Code Ann. § 541.001 et seq ("**TDPSA"**); (xviii) the Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq ("**UCPA"**); (xix) the Washington "My Health My Data" Act, Wash. Rev. Code § 19.373.005 et seq., and Nev. Rev. Stat. § 603A, as amended by Nevada S.B. 370 (together, the "**Washington and Nevada Consumer Health Data Laws**"); and (xx) the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 et seq. (SB 1392) ("**VCDPA**"). All as amended or superseded from time to time and including any implementing regulations and amendments thereto.

Any other terms that are not defined herein shall have the meaning provided under the Agreement or applicable Data Protection Laws. A reference to any term or section of the Data Protection Laws means the version as amended. Any references to the GDPR in this DPA shall mean the GDPR or UK GDPR depending on the applicable Law.

2. ROLES AND DETAILS OF PROCESSING

2.1. The parties agree and acknowledge that under the performance of their obligations set forth in the Agreement, and with respect to the Processing of Customer Data, and according to the applicable Data Protection Laws, Akeyless is acting as a Data Processor and Customer is acting as a Data Controller. Without derogating from the generality of the above, specifically, for the purpose of the Israeli Data Protection

Laws, the Akeyless shall Process Customer Data as the Holder on behalf of Customer as the Controller. Notwithstanding the above, in case the processing of the Personal Data is conducted under Customer's role as a Data Processor, the Akeyless shall be deemed a Sub-Processor.

2.2. Each party shall be individually and separately responsible for complying with the obligations that apply to such party under applicable Data Protection Law. The Customer shall be exclusively responsible to ensure its Instructions are compliant with applicable Data Protection Laws and enable a lawful Processing of Customer Data, including by obtaining any required consent and providing any required disclosures under applicable Data Protection Laws.

2.3. The subject matter and duration of the Processing carried out by the Processor on behalf of the Controller, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are described in **Annex I** attached hereto.

2.4. If any Sensitive Data or Special Categories of Personal Data or Highly Sensitive Data is processed (as those terms are defined under Data Protection Laws), including, any information that constitutes "consumer health data" under the CTDPA or the Washington and Nevada Consumer Health Data Laws or any information that constitutes "protected health information" under the Health Insurance Portability and Accountability Act of 1996, 5 U.S.C. § 553 et seq., together with any amending legislation and any regulations promulgated thereunder or any Personal Data that is deemed by US regulatory authorities as meriting sensitive treatment under US Data Protection Laws or U.S. state or federal consumer protection laws such as financial information, demographic information, credit scores, etc., it is Customer's responsibility to inform Akeyless of such processing, and ensure additional contractual obligations are met, if needed and applicable. For avoidance of doubt, Akeyless does not monitor, and review Customer Data processed according to this DPA, and may not be aware of any sensitivity within Customer Data.

3. PROCESSING OF PERSONAL DATA

3.1. Akeyless represents and warrants that it shall Process Customer Data, on behalf of the Customer, solely for the purpose of providing the Service, all in accordance with Customer's Instructions under the Agreement and this DPA. Notwithstanding the above, in the event Akeyless is required under applicable laws, including Data Protection Law or any union or member state regulation, to Process Customer Data other than as instructed by Customer, Akeyless shall make reasonable efforts to inform the Customer of such requirement prior to Processing such Customer Data, unless prohibited under applicable law.

3.2. Akeyless hereby certifies it understands the rules, requirements and definitions under applicable Data Protection Laws, and shall not: (i) Sell or Share the Customer Data; (ii) retain, use or disclose the Customer Data for any purpose other than for a Business Purpose specified in the Agreement; (iii) receive or Process any Personal Information as consideration for any Services it provides to the Customer; or (iv) combine the Customer Data with other Personal Data that it receives from, or on behalf of another customer.

3.3. Akeyless shall comply with the requirements set forth under applicable Data Protection Laws with regards to processing of de-identified data.

3.4. Akeyless shall inform Customer without undue delay in the event that, according to Akeyless's reasonable discretion, any of Customer's Instructions infringes applicable laws, and Akeyless shall have the right to immediately cease and suspend any such Processing activity related to the infringing Instruction.

3.5. Akeyless shall notify the Customer if it determines that it can no longer meet its obligations under this DPA or applicable Data Protection Law.

3.6. Akeyless shall provide reasonable cooperation and assistance to the Customer in ensuring compliance with its obligation to carry out data protection impact assessments and prior consultations with Supervisory Authorities or other competent data privacy authorities to the extent required under applicable Data Protection Laws (including data protection impact assessments and consultations with regulatory authorities), provided that Akeyless shall only be required to assist as for information which is reasonably available to Akeyless.

3.7. Where applicable, Akeyless shall assist the Customer in ensuring that Customer Data Processed is accurate and up to date, by informing the Customer without delay if it becomes aware of the fact that the Customer Data it is processing is inaccurate or has become outdated.

3.8. Akeyless shall ensure: (i) the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process Customer Data; and (ii) that persons authorized to Process the Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. DATA SUBJECTS RIGHTS AND LEGAL REQUEST

4.1. It is agreed that where Akeyless receives a request from a Data Subject for exercising a Data Subject's rights or from an applicable authority in respect of Customer Data, where applicable, Akeyless will notify the Customer of such request without undue delay and direct the Data Subject or the applicable authority to the Customer in order to enable the Customer to respond directly to the Data Subject's or the applicable authority's request, unless otherwise required under applicable laws.

4.2. Parties shall provide each other with commercially reasonable cooperation and assistance in relation to the handling of and responding to Data Subject's or applicable authority's request, to the extent permitted under Data Protection Law, including such request under the Data Privacy Framework. Akeyless shall provide Customer with cooperation and assistance mentioned above provided that the Customer cannot reasonably fulfill such obligations independently with the help of information available in the documentation, the website or any other self-service feature provided by Akeyless.

5. SUB-PROCESSING

5.1. The Customer provides general authorization for Akeyless to engage third party data Processors ("**Sub-Processor**") to Process Customer Data. The Customer specifically authorizes Akeyless to engage and appoint such Sub-Processors as listed in **Annex III**, to Process Customer Data, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf.

5.2. Akeyless may engage an additional or replace an existing Sub-Processors to Process Customer Data, subject to the provision of a thirty (30) days prior notice of its intention to do so to the Customer (such notice can be provided through the Customer account or through an email correspondence) ("**Notice**" and "**Notice Period**" respectively). In case the Customer has not objected to the adding or replacing of a Sub-Processor within Notice Period, such Sub-Processor shall be deemed approved by the Customer. In the event the Customer objects to the adding or replacing of a Sub-Processor, within such Notice Period, Akeyless may, under Akeyless' sole discretion, suggest the engagement of a different Sub-Processor for the same course of services, or otherwise enable the Customer to terminate the Agreement where the Services cannot be reasonably provided under such circumstances, without liability to Customer.

5.3. Akeyless shall, where it engages any Sub-Processor, impose, through a legally binding contract between Akeyless and the Sub-Processor, data protection obligations that are no less onerous than, and provide at least the same level of protection as, those set out in this DPA. Akeyless shall ensure that such contract will require the Sub-Processor to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Laws. Sub-processors shall be obligated, contractually, to reasonably cooperate with Akeyless, the Customer or an applicable regulatory authority in the event of an investigation or Security Incident.

5.4. Akeyless shall remain responsible to the Customer for the performance of the Sub-Processor's obligations in accordance with this DPA.

6. TECHNICAL AND ORGANIZATIONAL MEASURES

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and without prejudice to any other security standards agreed upon by the parties, Akeyless shall protect the security, confidentiality, integrity and availability of Customer Data and protect it against Security Incident.

6.2. Current technical and organizational measures implemented and maintained by Akeyless are further detailed in **Annex II** to this DPA, as updated from time to time (provided that any such amendments will not have a material negative effect on the level of protection provided to Customer Data).

7. SECURITY INCIDENT

7.1. Akeyless will notify the Customer without undue delay, no later than 72 hours, upon becoming aware of any Security Incident involving the Customer Data. Akeyless' notification regarding or response to a Security Incident under this Section 7 shall not be construed as an acknowledgment by Akeyless of any fault or liability with respect to the Security Incident.

7.2. Akeyless will: (i) take reasonably necessary steps to remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) upon Customer request, co-operate with the Customer and provide the Customer with such reasonable assistance and information in connection with the containment, investigation, remediation or mitigation of the Security Incident, including, where applicable, obligation to notify the affected Data Subjects. Upon Customer's request and taking into account the nature of the Processing and the information available to Akeyless, Akeyless will provide a report or written notice detailing the Security Incident, the affected Personal Data and Data Subjects.

8. AUDIT RIGHTS

8.1. Akeyless shall maintain accurate written records of any and all the Processing activities of any Customer Data carried out under this DPA its compliance with its obligations under this DPA, and shall make such records available to the Customer upon Customer's thirty (30) days prior written request, however no more than once per twelve (12) months of engagement ("**Audit Reports**"). A summary of the ISO27001/ISO27701 certification, SOCII report or recent penetration tests, as well as information provided through Customer's questionnaire shall be defined as a sufficient Audit Report. The Audit Report provided shall be considered Akeyless' Confidential Information and shall be subject to the corresponding confidentiality obligations under the Agreement or require signing a non-disclosure agreement.

8.2. In the event the Audit Report is reasonably determined as not sufficient for the purpose of demonstrating compliance, Akeyless shall make available, solely upon prior reasonable written notice and no more than once per calendar year, to a reputable auditor nominated by the Customer, information necessary to reasonably demonstrate compliance with this DPA or where required by Applicable Data Protection Law or an applicable authority, and shall allow for audits, including inspections, by such reputable auditor solely in relation to the Processing of the Customer Data ("**Audit**") in accordance with the terms and conditions hereunder. The auditor shall be subject to standard confidentiality obligations (including towards third parties). Akeyless may object to an auditor appointed by the Customer in the event Akeyless reasonably believes the auditor is not suitably qualified or is a competitor of Akeyless. Customer shall bear all expenses related to the Audit and shall (and ensure that each of its auditors shall) over the course of such Audit, ensure that the Audit is conducted during regular business hours, and avoid causing any damage, injury or disruption to Akeyless' premises, equipment, personnel and business while its personnel are on those premises in the course of such Audit. Akeyless shall agree to an Audit solely under the following terms: (i) a thirty (30) day prior written notice was provided; and (ii) restrict its findings to only to information relevant to Customer Data or an applicable Security Incident.

8.3. Nothing in this DPA will require Akeyless to either disclose to Customer or its third-party auditor, or to allow Customer or its third-party auditor to access: (i) any data of any other Akeyless' customer or Akeyless's internal data including without limitation data processed in Akeyless's role as a Controller; (ii) Akeyless' internal accounting or financial information; (iii) any trade secret of Akeyless or its Affiliates; (iv) any information that, in Akeyless' reasonable opinion, could compromise the security of any Akeyless' systems or cause any breach of its obligations under applicable law or its security, privacy or confidentiality obligations to any third party; or (v) any information that Customer or its third-party auditor seeks to access for any reason other than the good faith fulfillment of Customer's obligations under the Data Protection Laws. No access to any part of Akeyless's IT systems or infrastructure (including, without limitation, any hands-on or intrusive testing) will be permitted.

9. CROSS BORDER PERSONAL DATA TRANSFERS

9.1. Akeyless participates in and certifies compliance with the Data Privacy Framework. As required by the Data Privacy Framework, Akeyless (i) provides at least the same level of privacy protection as is required by the Data Privacy Framework Principles; (ii) will notify Customer if Akeyless makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) will, upon written notice, take reasonable and appropriate steps to remediate any unauthorized Processing of Personal Data.

9.2. Customer acknowledges and agrees that for the provisions of the Services, Akeyless may Process, including transfer, Customer Data to various jurisdictions where Akeyless, its affiliates or Sub-Processors operate. Akeyless will ensure that transfers are made in compliance with Data Protection Laws.

9.3. Where European Data Protection Laws apply:

9.3.1. Akeyless will not transfer Customer Data originating from the EEA, the UK or Switzerland, to any country or recipient not recognized as providing an adequate level of protection for such Personal Data (within the meaning of the European Data Protection Law), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Laws. Such measures may include (without limitation) (i) transferring such Customer Data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including to an Adequate Country or data privacy and transfer frameworks; (ii) to a recipient that has achieved binding corporate rules authorization in accordance with applicable Data Protection Law; or (iii) to a recipient that has executed the Standard Contractual Clauses.

9.3.2. When Customer and Akeyless, or Akeyless and or its Sub-Processor rely on the Standard Contractual Clauses to facilitate a transfer to a third country the following shall apply:

1. For Transfer of Customer Data from the EEA the EU SCC shall apply and completed as follows: **(1)** Module II (Controller to Processors) or

Module III (Processor to Processor) will apply; **(2)** In Clause 7 the optional docking clause will not apply; **(3)** In Clause 9, option 2 (general written authorization) shall apply for the Sub-Processors listed under **Annex III** and the method for appointing Sub-Processor shall be as set forth in the Sub-Processing Section of the DPA; **(4)** In Clause 11, the optional language will not apply, and Data Subjects shall not be able to lodge a complaint with an independent dispute resolution body; **(5)** In Clause 17, option 1 shall apply, and the EU SCC shall be governed by the law of the Republic of Ireland; **(6)** In Clause 18(b) the parties choose the competent courts of the Republic of Ireland, as their choice of forum and jurisdiction; **(7) Annex I(A) of the EU SCC** is completed as follows: Customer is the Data Exporter, Akeyless is the Data Importer, the parties' contact details are as completed under the Agreement; **Annex I(B) of the EU SCC** is completed as set out in Annex I of this DPA; **Annex I(C) of the EU SCC** shall identify the competent supervisory authority/ies as the supervisory authority Republic of Ireland; **(8) Annex II of the EU SCC** is deemed completed with the information set out in Annex II of this DPA; **(9) Annex III of the EU SCC** shall be completed with the list of Sub-Processors set out in Annex III of this DPA.

2. For transfer of Customer Data from the UK, the UK SCC shall apply and completed as follows: **(1) Table 1** shall be completed as set forth in section (i)(7) above; **(2) Table 2** shall be completed as set forth in Section (i)(1) – (i)(4) above; **(3) Tables 3** shall be completed as follows: **Annex 1A** shall be completed with relevant information as set out in Section (i)(7) above; **Annex 1B** shall be completed with relevant information as set out in **Annex I** of this DPA; , **Annex II** shall be completed with relevant information as set out in Annex II of this DPA; **Annex III** shall be completed with the list of sub-processors set out in Annex III of this DPA; **(4) Table 4** shall be completed with the "neither party" option; and **(5)** Any conflict between the terms of the EU SCC and the UK SCC will be resolved in accordance with Section 10 and Section 11 of the UK SCC.

3. For transfer of Customer Data from Switzerland, the Swiss SCC shall apply in with following modifications (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

10. TERM, TERMINATION AND CONFLICT

10.1. This DPA shall be effective as of the Effective Date (as defined in the Agreement) and shall remain in force until the Agreement terminates or as long as Akeyless Processes Customer Data.

10.2. Akeyless shall be entitled to terminate this DPA or cease the Processing of Customer Data in the event that Processing of Customer Data under the Customer's Instructions or

this DPA infringe applicable legal requirements, provided Customer did not provide updated Instructions to cure such infringement within ten (10) days from receiving applicable notice from Akeyless. Alternately, Akeyless may, in its sole discretion, suspend the Processing of the Customer Data until such infringement is cured without liability to the Customer and without prejudice to any fees incurred by Customer prior to suspension date.

10.3. Following the termination or expiration of this DPA, Akeyless shall, at the choice of the Customer, delete or return all Customer Data Processed on behalf of the Customer and certify to the Customer that it has done so. Until the Customer Data is deleted or returned, the parties shall continue to ensure compliance with this DPA. Customer's choice shall be provided in writing to Akeyless, following effect of termination. Notwithstanding the foregoing, Akeyless may retain Customer Data (i) as required by applicable laws; or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Akeyless will maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to retained Customer Data and not further Process it except for those purposes that justify further retention of Customer Data.

10.4. In the event of a conflict between the terms and conditions of this DPA and the Agreement, this DPA shall prevail. For the avoidance of doubt, in the event Standard Contractual Clauses have been executed between the parties, the terms of the Standard Contractual Clauses shall prevail over those of this DPA.

ANNEX I

DETAILS OF PROCESSING

This Annex includes certain details of the Processing of Customer Data as required under the Data Protection Laws.

Categories of Data Subjects:

As uploaded by Customer while using the Services.

Categories of Personal Data processed:

As uploaded by Customer while using the Services.

Special Categories of Personal Data:

None. Customer is specifically prohibited from providing Akeyless any Sensitive Data or Special Categories of Data, unless agreed in writing by Akeyless.

Nature of the processing:

Collection, storage, organization, communication, transfer, host and other types of Processing for the purpose of providing the Services as set out in the Agreement.

Purpose(s) of Processing:

To provide the Service.

Retention Period:

For as long as is necessary to provide the Service by Akeyless; provided there is no legal obligation to retain the Customer Data post termination or unless otherwise requested by the Customer.

Process Frequency:

Continuous basis

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES

Please review Akeyless' security policy here and here to learn more regarding the technical and organizational measures implemented by it in order to ensure an appropriate level of security for its Processing of Customer Data.

ANNEX III

LIST OF SUB-PROCESSORS

As of the effective date above, Akeyless uses the following sub-processors: https://www.akeyless.io/list-of-sub-processors/