CUSTOMER DATA PROCESSING ADDENDUM FOR SAAS PRODUCTS

This Data Processing Addendum ("**DPA**") forms an integral part of the Agreement ("**Main Agreement**") between Varonis Systems, Inc. and/or its subsidiaries. (**"Company**") and between the counterparty agreeing to these terms ("**Customer**"; each "**Party**" and together "**Parties**") and applies to the extent that Company processes Personal Data on behalf of the Customer, in the course of its performance of its obligations under the Main Agreement. By accepting the Main Agreement the Customer accepts the terms in this DPA.

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

1. **Definitions**

1.1 "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

1.2 **"Data Protection Law**" means, as applicable, any and all domestic and foreign laws, rules, directives and regulations, on any local, provincial, state, federal or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (as amended, and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"); the Data Protection Act 2018 and the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); Singapore's Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**") and Personal Data Protection Regulations 2021, and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**") and the regulation enacted thereunder including the California Privacy Rights and Enforcement Act of 2020 ("CPRA"); Australia's Privacy Act 1988 including the Australian Privacy Principles ("APPs"); the Virginia Consumer Data Protection Act, Va. Civ. Code § 59.1 ("**VCDPA**") (together with the CCPA and CPRA ,"**US Data Protection Laws**"), including any amendments or replacements to the foregoing.

1.3 "**Data Subject**" means an individual to whom Personal Data relates. Where applicable, Data Subject shall be deemed as a "**Consumer**" as this term is defined under the US Data Protection Laws and as an "Individual", as this term is defined under the PDPA.

1.4 "**DPF"** means the EU-U.S. Data Protection Framework, pursuant to the European Commission Implementing Decision of 10.7.2023 ("**EU-U.S. DPF**"), and, as applicable, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework.

1.5 **"EEA**" means those countries that are member of the European Economic Area.

1.6 "**Permitted Purposes**" mean any purposes in connection with Company performing its obligations under the Main Agreement.

1.7 "**Security Incident**" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. For the avoidance of doubt, any Personal Data Breach (as defined under Data Protection Laws) will comprise a Security Incident.

1.8 "**Security Measures**" mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of Company's business, the level of sensitivity of the data collected, handled and stored, and the nature of Company's services, as further described in Annex 2.

1.9 "**Standard Contractual Clauses**" mean (a) with respect to the transfers to which the GDPR applies - Module Two or Module Three, as applicable, of 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 from June 4th 2021, as available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en; and
(b) with respect to transfers to which the UK GDPR applies - the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018, currently available here: https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf; both (a) or (b) above, as applicable, are incorporated herein by reference.

1.10 "**Sub-Processor(s)**" mean any Affiliate, agent or assignee of Company that may process Personal Data pursuant to the terms of the Main Agreement, and any unaffiliated processor, vendors or service provider engaged by Company.

1.11 "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, which was entered into force on 21 March, 2022.

1.12 The terms "**Controller**", "**Personal Data**", "**Processor**", "**Process**" and "**Processing**" shall have the meanings ascribed to them in the Data Protection Law, as applicable.

2. Application of this DPA

2.1 This DPA will only apply to the extent all of the following conditions are met:
(A) Company processes Personal Data that is made available by the Customer in connection with the Main Agreement (whether directly by the Customer or indirectly by a third party retained by and operating for the benefit of the Customer);
(B) The Data Protection Law apply to the processing of Personal Data.

2.2 This DPA will only apply to the services for which the Parties agreed to in the Main Agreement ("**Services**"), which incorporates the DPA by reference.

3. Parties' Roles

3.1 In respect of the Parties' rights and obligations under this DPA regarding the Personal Data, the Parties hereby acknowledge and agree that the Customer is the Controller (as well as, as applicable, the Business, as the term is defined under US Data Protection Laws, or the Organization, as this term is defined under the PDPA) and Company is a Processor (as well as, as applicable, the Service Provider, as this term is defined under US Data Protection Laws, or the Data Intermediary, as this term is defined under the PDPA), or if the Personal Data processed by the Company in accordance with the Main Agreement is of a Customer acting as Processor of behalf of a third party, then the Company shall be the Sub Processor. Accordingly:
(A) Company agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA;

(B) The Parties acknowledge that the Customer discloses Personal Data to Company only for the performance of the Services and that this constitutes a valid business purpose for the processing of such data.

3.2 If Customer is a Processor, Customer warrants to Company that Customer's instructions and actions with respect to the Personal Data, including its appointment of Company as Sub-Processor and concluding the Standard Contractual Clauses, have been authorized by the relevant controller.

3.3 Notwithstanding anything to the contrary in the DPA, Customer acknowledges that Company shall have the right to Process certain Personal Data collected in the context of providing the Services, for its legitimate business purposes as a Controller, such as:

(A) the provision and operation of its Services, administrating the business and/or contractual relationship with the Customer, billing, audit and recordkeeping purposes, as well as for account management, security, establishment or exercise of legal claims and protection against fraudulent or illegal activity.

(B) for the purpose of improving customers' threat protection. If the Customer wishes that the Company uses only aggregated and/or anonymized information for such purposes, Customer is solely responsible to choose to opt-out of non-aggregated and/or non-anonymized processing in the management interface in the Customer's product. The Company may use aggregated and/or anonymized information for any purpose, subject to the confidentiality obligation in the Main Agreement. For the avoidance of doubt, non-aggregated and non-anonymized data referred to in this section shall be retained for the same period as the Personal Data.

4. **Compliance with Laws**

4.1 Each Party shall comply with its respective obligations under the Data Protection Law.

4.2 Company shall provide reasonable cooperation and assistance to Customer in relation to Company's processing of Personal Data in order to allow Customer to comply with its obligations as a Data Controller under the Data Protection Law.

4.3 Company agrees to notify Customer promptly if it becomes unable to comply with the terms of this DPA and take reasonable and appropriate measures to remedy such non-compliance.

4.4 Throughout the duration of the DPA, Customer agrees and warrants that:

(A) Personal Data has been and will continue to be processed by Customer in accordance with the relevant provisions of the Data Protection Law;

(B) Customer is solely responsible for determining the lawfulness of the data processing instructions it provides to Company and shall provide Company only instructions that are lawful under Data Protection Law;

(C) The processing of Personal Data by Company for the Permitted Purposes, as well as any instructions to Company in connection with the processing of the Personal Data ("**Processing Instructions**"), has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law; and that

(D) The Customer has informed Data Subjects of the processing and transfer of Personal Data pursuant to the DPA and obtained the relevant consents or lawful grounds thereto (including without limitation any consent required in order to comply with the Processing Instructions and the Permitted Purposes).

5. **Processing Purpose and Instructions**

5.1 The subject matter of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, shall be as set out in the Main Agreement, or in the attached Annex 1, which is incorporated herein by reference.

5.2 Company shall Process Personal Data only for the Permitted Purposes and in accordance with Customer's written Processing Instructions (unless waived in a written requirement), the Main Agreement and the Data

Protection Law, unless Company is otherwise required by law to which it is subject (and in such a case, Company shall notify Customer of that legal requirement before Processing, provided that the Company is not legally prohibited from doing so).

5.3 To the extent that any Processing Instructions may result in the Processing of any Personal Data outside the scope of the Main Agreement and/or the Permitted Purposes, then such Processing will require prior written agreement between Company and Customer, which may include any additional fees that may be payable by Customer to Company for carrying out such Processing Instructions.

5.4 Company shall not retain, use or disclose the Personal Data for any purpose other than for the specific purpose of performing the Services or outside of the direct business relationship between the Parties, including for a commercial purpose other than providing the Services, except as required under applicable laws, or as otherwise permitted under Data Protection Law. Company's performance of the Services may include disclosing Personal Data to Sub-Processors where this is necessary for the performance of the Services. The Company certifies that it, and any person receiving access to Personal Data on its behalf, understand the restrictions contained herein.

6. Reasonable Security and Safeguards

6.1 Company represents, warrants, and agrees to use Security Measures (i) to protect the availability, confidentiality, and integrity of any Personal Data Processed by Company in connection with the Main Agreement, and (ii) to protect such data from Security Incidents. Such Security Measures include, without limitation, the security measures set out in Annex 2.

6.2 The Security Measures are subject to technical progress and development and Company may update or modify the Security Measures from time to time provided that such updates and modifications do not result, in the Company's discretion, in the material degradation of the overall security of the services procured by Customer. The Company will provide notice (in the Company's portal for customers) of material changes in Security Measures, when possible, at least 10 days before the change will take effect.

6.3 Company shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who Processes Personal Data. Company shall ensure that persons authorized to Process Personal Data are under an appropriate obligation of confidentiality.

7. Security Incidents

7.1 Upon becoming aware of a Security Incident, Company will notify Customer without undue delay and will provide reasonable information relating to the Security Incident as reasonably requested by Customer. Company will use reasonable endeavors to assist Customer in mitigating, where possible, the adverse effects of any Security Incident as relates to Company's products and services.

8. Security Assessments and Audits

8.1 Company audits its compliance with data protection and information security standards on a regular basis. Such audits are conducted by Company's internal audit team or by third party auditors engaged by Company.

8.2 At Customer's written request, and subject to obligations of confidentiality, Company may satisfy the requirements set out in this section by providing Customer with Company's SOC 2 Type II report, so that Customer can reasonably verify Company's compliance with its obligations under this DPA. Customer shall rely on the SOC 2 Type II report for validation of proper information security practices and shall not have an additional right to audit Company's compliance unless such right is specifically granted to Customer under applicable law. The foregoing shall not apply solely in the case of a Security Breach resulting in a material business impact to Customer or in connection to a Supervisory Authority specific request. In such event,

Customer shall provide Company with 30 days prior written notice (insofar as possible) and the details of any 3rd party auditor on its behalf, for approval.

9. **Cooperation and Assistance**

9.1 If Company receives any requests from individuals or applicable data protection authorities relating to the Processing of Personal Data under the Main Agreement, including requests from individuals seeking to exercise their rights under Data Protection Law, Company will promptly redirect the request to Customer. Company will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. The Customer is responsible for verifying that the requestor is the data subject whose information is being sought or its duly authorized representative. Company bears no responsibility for information provided in good faith to Customer in reliance on this subsection.

9.2 If Company receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, Company shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. It is hereby clarified however that if no such response is received from Customer within three (3) business days (or otherwise any shorter period as dictated by the relevant law or authority), Company shall be entitled to provide such information.

9.3 Notwithstanding the foregoing, Company will cooperate with Customer with respect to any action taken by it pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed Personal Data. Customer shall cover all costs incurred by Company in connection with its provision of such assistance.

9.4 Upon reasonable notice, Company shall:

(A) Taking into account the nature of the Processing, provide reasonable assistance to the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising Data Subject's rights, at Customer's expense;

(B) Provide reasonable assistance to the Customer in ensuring Customer's compliance with its obligation to carry out data protection impact assessments or prior consultations with data protection authorities with respect to the processing of Personal Data, provided, however, that if such assistance entails material costs or expenses to Company, the Parties shall first come to agreement on Customer reimbursing Company for such costs and expenses.

10. **Use of Sub-Processors**

10.1 Customer provides a general authorization to Company to appoint Sub Processors in accordance with this Clause.

10.2 Company may continue to use those Sub Processors already engaged by Company as at the date of this DPA, as specified in Annex 3, subject to Company, in each case as soon as practicable, meeting the obligations set out in this DPA.

10.3 Company can at any time appoint a new Sub-Processor provided that the Company provides notice (in the Company's portal for customers), at least 10 days before the appointment will take effect, and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Sub-Processor's non-compliance with Data Protection Law. If, in Company's reasonable opinion, such objections are legitimate, Company shall either refrain from using such Sub-Processor in the context of the processing of Personal Data or shall notify Customer of its intention to continue to use the Sub-Processor. Where Company notifies Customer of its intention to continue to use the Sub-Processor in these circumstances and does not provide the Customer with any other alternative, Customer

may, by providing written notice to Company, terminate the Services in the Main Agreement that require the Processing by that Sub-Processor.

10.4 With respect to each Sub-Processor, Company shall ensure that the arrangement between Company and the Sub-Processor is governed by a written contract, including terms which offer at least the same level of protection as those set out in this DPA and meet the requirements of Data Protection Law, including the requirements of article 28(3) of the GDPR, as applicable;

10.5 Company will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Company to breach any of its obligations under this DPA.

10.6 Company will only disclose Personal Data to Sub-Processors for the specific purposes of carrying out the Services on Company's behalf.

11. **Transfer of EEA or UK Residents' Personal Data outside the EEA or UK**

11.1 The Company has certified with the DPF and shall comply with its principles with respect to any personal data transfers outside the EU, UK or Switzerland, to the US. To the extent that Company Processes Personal Data outside the EEA, UK or an Approved Jurisdiction, which is not subject to Company's DPF certification, then the Parties shall be deemed to enter into the Standard Contractual Clauses, subject to any amendments contained in Exhibit A, in which event the Customer shall be deemed as the Data Exporter and the Company shall be deemed as the Data Importer (as these terms are defined therein).

11.2 Company may transfer Personal Data of residents of the EEA or UK outside the EEA or UK ("**Transfer**"), only subject to the following:

(A) The Transfer is necessary for the purpose of Company carrying out its obligations under the Main Agreement, or is required under applicable laws; and

(B) The Transfer is done: (i) to an Approved Jurisdiction, or (ii) subject to appropriate safeguards (for example, through the use of the Standard Contractual Clauses, or other applicable frameworks), (iii) in accordance with the DPF principles, or (iv) in accordance with any of the exceptions listed in the Data Protection Law (in which event, Customer will inform Company which exception applies to each Transfer and will assume complete and sole liability to ensure that the exception applies).

11.3 Annex 3 to this DPA provides a list of countries to which the Personal Data will be transferred by Company under this DPA.

12. **Data Retention and Destruction**

12.1 Company will only retain Personal Data for the duration of the Main Agreement or as required to perform its obligations under the Main Agreement, for the establishment or exercise of legal claims, or as otherwise required to do so under applicable laws or regulations. The retention policy can be found in the Company's Software Privacy Policy - https://www.varonis.com/software-privacy-policy. Following expiration or termination of the Main Agreement, Company will delete or return to Customer all Personal Data in its possession as provided in the Main Agreement, except to the extent Company is required under applicable laws to retain the Personal Data. The applicable terms of this DPA will continue to apply to such Personal Data. This section shall not apply to the activities that are the subject matter of section 3.3(b) herein.

13. **Obligations under US Data Protection Laws**

13.1 To the extent that Company processes Personal data of which is subject to the US Data Protection Laws:

13.1.1 Company shall not sell or share such Personal Data (as the terms "sell" and "share" are defined under US Data Protection Laws).

13.1.2 Company is prohibited from retaining, using or disclosing such Personal Data for a commercial purpose other than providing the service to the Customer under the Main Agreement and from retaining, using or disclosing such Personal Data outside of the Main Agreement, including but not limited to combining the Personal data for cross-context behavioral advertising purposes.

Company acknowledges and understands its obligations under this clause, and will comply with them.

14. **General**

13.1 Any claims brought under this DPA will be subject to the terms and conditions of the Main Agreement, including the exclusions and limitations set forth in the Main Agreement.

13.2 In the event of a conflict between the Main Agreement (or any document referred to therein) and this DPA, the provisions of this DPA shall prevail.

13.3 Company may change this DPA if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the Company as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party's rights to Process Personal Data; or (iii) have a material adverse impact on Customer, as reasonably determined by Company.

13.4 If Company intends to change this DPA, and such change will have a material adverse impact on Customer, as reasonably determined by Company, then Company will inform Customer (in the Company's portal for customers) at least 10 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

Exhibit A - SCC

1. If Customer is a Controller – the Parties shall be deemed to enter into the Controller to Processor Standard Contractual Clauses (Module Two); if Customer is a Processor – the Parties shall be deemed to enter into the Processor to Processor Standard Contractual Clauses (Module Three).

2. This Exhibit A sets out the Parties' agreed interpretation of their respective obligations under Module Two or Module Three of the Standard Contractual Clauses (as applicable).

3. The Parties agree that for the purpose of transfer of Personal Data between the Customer (Data Exporter) and the Company (Data Importer), the following shall apply:

   3.1. Clause 7 of the Standard Contractual Clauses shall not be applicable.

   3.2. In Clause 9, option 2 shall apply.

   3.3. In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.

   3.4. In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by the laws of the Republic of Ireland. Notwithstanding the forgoing, the UK SCCs shall be governed by the laws of England and Wales.

   3.5. In Clause 18(b) the Parties choose the courts of Dublin Ireland, as their choice of forum. Where the UK SCCs apply, the courts of London, England shall have exclusive jurisdiction.

4. The Parties shall complete Annexes I–II below, which are incorporated in the Standard Contractual Clauses by reference.

5. To the extent the UK Addendum applies, the following shall apply:

   5.1. All the information provided under the Standard Contractual Clauses shall apply to the UK Addendum with the necessary changes per the requirement of the UK Addendum. Annexes 1A, 1B and 2 to the UK Addendum shall be replaced with the Annexes attached hereto, respectively.

   5.2. In Table 4 of the UK Addendum, either party may terminate the agreement in accordance with section 19 of the UK Addendum.

   5.3. By entering into this Data Protection Agreement, the Parties hereby agree to the formatting changes made to the UK Addendum.

ANNEX I TO DPA

This Annex forms an integral part of the DPA.

CATEGORIES OF DATA SUBJECTS:

The Personal Data transferred concern the following categories of Data Subjects (please specify):

Individuals whose personal data is on Customer's systems or environments that are monitored by Company's products.

CATEGORIES OF PERSONAL DATA:

Personal Data that is included in the metadata scanned by Varonis software, such as: names, email addresses, IP addresses, information that is included in file and folder names.

SPECIAL CATEGORIES OR SENSITIVE CATEGORIES OF PERSONAL DATA (AS APPLICABLE):

No "sensitive" or "special categories" of Personal Data (as these terms are defined under applicable Data Protection Law) are expected. Customer may, at its sole discretion, opt to share such Personal Data while using the Services. Customer is solely responsible for informing Company in such cases, and for obtaining any lawful consent and for providing disclosure to Data Subjects, as applicable.

THE FREQUENCY OF THE TRANSFER

Continuous

NATURE OF THE PROCESSING

x Collection

x Recording

x Organization or structuring

x Storage

x Adaptation or alteration

x Retrieval

x Consultation

x Disclosure, dissemination or otherwise making available

x Analysis

☐ Erasure or destruction

☐ Other: _____

PURPOSE OF THE TRANSFER AND FURTHER PROCESSING

As defined in the Main Agreement. The parties may mutually agree in writing to amend this Annex I.

RETENTION PERIOD

Personal Data will be retained as detailed in the Main Agreement and the DPA.

ANNEX 2 TO DPA

This Annex forms part of the DPA and describes the technical and organisational security measures implemented by the data importer.

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, the Company shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

More specifically, data Company's security controls shall include:

Domain	Practices
Information Security Policy	○ Varonis maintain written privacy and security policies, which is consistent in material respects with the requirements of this document and with prevailing industry standards. Such policies support and ensure the confidentiality, integrity, and availability of the Data. Varonis hereby warrants and undertakes that it has and that it will maintain throughout the term of the Agreement a written, comprehensive information security program that complies with applicable laws and information security standards. ○ Policies are reviewed and approved by management periodically. ○ Information Security roles and responsibilities are documented and communicated to the relevant personnel. ○ Varonis designated an Information Security Officer who is operationally responsible for assuring that Varonis complies with security policies, and applicable standards and regulations.
Access Control	○ All Varonis system that handles customer data are secured with the described security measures. ○ Access to customer data is managed through a secure authentication. A formal user registration and de-registration procedures for granting and revoking access to information systems and services is maintained. ○ Access to customer data is provided on the need to know basis. Access by Varonis personnel who no longer requires access to perform the Services is terminated. ○ Formal management review of user access rights is performed at regular intervals. ○ Password policy is enforced to company networks and assets. Password Policy include, and not limited to the settings of password age, length, history, complexity requirements, and account lockout duration. ○ Session time-out is enforced on company assets. ○ Administrative and privileged access is restricted to trained and authorized employees of the Data Processor.

Operations Security	○ Information backup is conducted regularly, to allow adequate recovery of information in cases of damage to the information or its systems. Backups are protected using industry best practices encryption, and access control. ○ Periodic restoration tests are performed for scoped data. ○ Varonis perform periodic technical vulnerability scans on networks, and applications that process, store, or transmit Customer's Data. Remediation of vulnerabilities is monitored and performed according to a defined procedure. ○ Malware protection is implemented on Varonis' assets to avoid malicious software gaining unauthorized access to Customer Data. ○ Changes to production infrastructure and networks are monitored and controlled though a change management process. Changes are reviewed and approved prior to implementation and recorded after it. ○ Audit logs recording user activities, exceptions, faults, and information security events are produced, kept, and monitored.
Cryptography	○ Varonis encrypt customer data that is transmitted over public networks, as well as implementing encryption of data at rest. ○ Strong and non-deprecated versions of encryption algorithms and key lengths are used and monitored. ○ Keys and secrets are maintained secured. Access to the Keys and secrets is limited to a minimal number of users on a need-to-know basis. ○ All keys are periodically rotated.

Physical and environmental security	○ Facilities and processing centers are equipped with physical security systems and monitoring as required by security standards (such as ISO/IEC 27001 and/or SOC 2 Type 2), local laws, and regulations. ○ Varonis limit physical access to its electronic information systems and the facilities in which they are housed, and safeguard those facilities against unauthorized physical access, tampering, and theft. ○ Clean desk policy is designed to prevent inadvertent disclosure of personal data. ○ Varonis validates that its cloud service providers maintain physical security policy that is aligned with security industry best-practices, and audited periodically by external third-party auditors (i.e., SOC 2, ISO27001)
Communications Security	○ Varonis applies the principle of least required access for allowed network communications. ○ All network communications are protected with confidentiality and integrity. ○ All network communications are monitored for security incidents Remote access to customers' data is established using a secure, and strong authenticated connection. ○ Restrictions are in be placed in front of externally exposed applications and endpoints.
System Acquisition, development, and maintenance	○ Varonis follows formal Secure Software Development cycle. ○ Rules for the secure software development and systems is established and applied to engineering within the organization. ○ Testing of security functionality is carried out during the development phases. ○ Acceptance testing programs and related criteria is established and maintained for systems, upgrades, and new versions.
Supplier Relationships	○ business arrangements with suppliers, involving their access to Varonis' information, systems and applications shall be based on a formal agreement, consisting of all necessary security and confidentiality relevant to the interaction between Varonis and the suppliers. ○ Technology service providers undergo a security risk assessment and approved by the CISO department. ○ Varonis ensure all suppliers which holds customer’s data are operating, and providing their service, at a security level that is no less stringent than those outlined in this document.

Information Security Incident Management	○ Varonis shall have an updated policy and procedures to assign responsibilities of Varonis personnel and identification of parties to be notified in case of an information security incident, is in place. Customers can report security incidents related to the scoped services to soc@varonis.com ○ Varonis is regularly monitoring security events and alerts from production systems to identify abnormal user and system behavior. ○ Varonis maintains a record of security breaches with sufficient information to allow customers to meet any of its own obligations under relevant data privacy and data security laws and other contractual obligations.
Business continuity management	○ Varonis has a procedure to rebuild cloud environment and recover customer data in case of a disaster causing a destruction before the time it was lost or destroyed. ○ Infrastructure capacity and applicable third-party services are regularly monitored to minimize service disruption. ○ Varonis ensures that all dependent cloud service providers have adequate measures for disaster recovery
Compliance	○ Periodically, Varonis will conduct an independent third-party review (such as ISO/IEC 27001 and/or SOC 2 Type 2) of its security policies, and procedures related to the Services provided to Customer. The list of certificates is available in the Trust Center.
Human Resources	○ New hire process is established and includes screening checks and employee's commitment to confidentiality for employees with access to customer data. ○ Employees undergo periodic security awareness training and are updated on procedures to report security incidents.
Asset Management	○ Asset inventory is maintained and includes ownership and labelling where applicable. ○ Policy for Acceptable use of assets is developed and implemented in accordance with industry best practices. ○ Restrictions are in place to prohibit data transfer to removable media. ○ Varonis ensures that its service providers maintain a secure disposal process when such data is no longer needed.

Annex 3 to DPA

Sub Processors

Service Providers

Name	Purpose of Processing	Location	Scope of processed PII
Microsoft services	Azure - Infrastructure and Platform as a Service (except DatAdvantage Cloud), DevOps App platforms (TFS) - Customer Support management and collaboration, Sentinel - Security information and event management, O365 and Teams - internal communication Generative AI infrastructure	Azure cloud – US, EU, UK, Australia or Canada, per customer choice Other services - US	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
AWS	Infrastructure Hosting Service (HIS) – only for DatAdvantage Cloud SES - Communication application	HIS - US, EU or Canada per customer initial choice of cloud locality SES - Per customer initial choice of cloud locality	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
DataDog (only for DatAdvantage Cloud)	Centralized platform for monitoring, visualizing, and alerting on data.	Per customer initial choice of cloud locality	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
Imperva	Web Application Firewall	Per customer initial choice of cloud locality	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
Cloud AMQP (except DatAdvantage Cloud)	Message Broker	Per customer initial choice of cloud locality	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
Box	Files from Varonis support, PS etc. that include logs that may contain PII	Per customer initial choice of cloud locality	Personal Data processed by Varonis as a result of Client's use of the Subscription Services.
Okta	Identity Management solution	US	Email of client's personnel accessing the system

Slack (only for DatAdvantage Cloud)	Messaging application	US	Email of client's personnel accessing the system
Salesforce	Support ticket management platform (not including files attached to tickets)	US	Email of client's personnel accessing the system

Varonis Group Entities

The following entities are members of the Company Group, and function as sub-processors to provide the services.

Entity Name	Entity Country
Varonis Systems, Inc.	USA
Varonis Systems Ltd.	Israel
Varonis Systems (Ireland) Limited	Ireland
Varonis France SAS	France
Varonis (UK) Limited	UK
Varonis Systems (Deutschland) GmbH	Germany
Varonis Systems (Netherlands) B.V.	The Netherlands and Belgium
Varonis Systems (Luxemburg) S.à r.l.	Luxemburg
Varonis Systems Australia Pty Ltd	Australia
Varonis Systems Corp	Canada
Varonis Singapore PTE Ltd.	Singapore