CUSTOMER DATA PROCESSING ADDENDUM FOR SAAS PRODUCTS

This Data Processing Addendum (this "**DPA**") forms an integral part of the agreement between Varonis Systems, Inc. and/or its subsidiaries (collectively, the "**Company**") and the counterparty agreeing to these terms (the "**Customer**"; each a "**Party**" and together "**Parties**") which governs the Customer's use of the Company's products and services (the "**Main Agreement**") 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 Laws**" mean any and all applicable 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 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**" or as "**Individual**", as these terms are defined under Data Protection Laws.

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 described in this DPA.

1.7 "**Personal Data**" means personal data, relating to an identified or identifiable natural person (as defined under the Data Protection Laws), processed by the Company on behalf of the Customer in accordance with the Main Agreement and this DPA.

1.8 "**Security Incident**" means breach of security leading to an 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.

1.9 "**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, that can be found in the following link: https://varon.is/securityschedule.

1.10 "**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 4, 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/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/; each (a) and (b) above, as applicable, is incorporated herein by reference.

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

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

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

2. Application of this DPA

2.1. This DPA will only apply to the extent the Company processes Personal Data in connection with the Main Agreement.

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 or the Organization, as such term is defined under Data Protection Laws,) and the Company is a Processor (as well as, as applicable, the Service Provider or the Data Intermediary, as such term is defined under Data Protection Laws), or if Personal Data processed by the Company in accordance with the Main Agreement is of a Customer acting as Processor on behalf of a third party, then the Company shall be the Sub Processor. Accordingly:

(A) The Company agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA; and

(B) The Parties acknowledge that the Customer discloses Personal Data to the Company only for the provision of the licenses and services as set forth in the Main Agreement, and that this constitutes a valid business purpose for the processing of such data.

3.2 If Customer is a Processor, the Customer represents and warrants to the 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 this DPA, the 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 follows:

(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 or anonymized information for such purposes, the Customer is solely responsible to choose

to opt-out of non-aggregated or non-anonymized processing in the management interface in the Customer's product. For the avoidance of doubt, non-aggregated or non-anonymized data referred to in this section shall be retained for the same period as the Personal Data in accordance with this DPA.

4. Compliance with Laws

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

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

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

4.4 For as long as this DPA is in effect, the Customer agrees and warrants that any Customers instructions to the 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 Laws.

5. Processing Purpose and Instructions

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

5.2 The Company will 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, this DPA 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 The Company shall not retain the Personal Data, use it or disclose it to third parties, except (a) as necessary to provide the Services in accordance with the Main Agreement and this DPA (including to Sub Processors in accordance with Section 10), (b) as instructed or agreed by the Customer, or (c) as required under applicable laws.

6. Security and Safeguards

6.1 The Company warrants that it uses Security Measures to (i) protect the availability, confidentiality, and integrity of any Personal Data Processed by the Company in connection with the Main Agreement, and (ii) protect such data from Security Incidents. Such Security Measures include, without limitation, the security measures set out in Annex 2, that can be found in the following link: https://varon.is/securityschedule.

6.2 The Security Measures are subject to technical progress and development, and the 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. The Company will provide notice (via the Company's customers portal) of material changes to the Security Measures, when possible, at least 10 days before such change takes effect.

6.3 The 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

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

8. Security Assessments and Audits

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

8.2 At Customer's written request, and subject to confidentiality obligations, the Company will satisfy the requirements set out in this section by providing the Customer with the Company's SOC 2 Type II report and shall respond to privacy and security questionnaires no more than once a year, so that the Customer can reasonably verify the Company's compliance with its obligations under this DPA. The Customer shall rely on the SOC 2 Type II report and the questionnaires for validation of proper information security practices and shall not have an additional right to audit Company's compliance unless such right is explicitly granted to Customer under Data Protection Law. The foregoing shall not apply solely in the case of a Security Incident resulting in a material business impact to Customer, or in connection to a Supervisory Authority specific request for an audit on the Services. In such event, the Customer shall, to the extent practicable, provide Company with 30 days' prior written notice and the details of any independent third-party auditor acting on its behalf, for the Company's prior approval (not to be unreasonably withheld).

9. Cooperation and Assistance

9.1 If the 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 the Data Protection Laws, the Company will promptly redirect the request to the Customer. The Company will not respond to such communication directly without the 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. The Company bears no responsibility for information provided in good faith to Customer in reliance on this subsection.

9.2 If the 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, the 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. The Customer shall cover all costs incurred by Company in connection with its provision of such assistance.

9.4 Upon reasonable notice, the Company shall:

(A) Taking into account the nature of the Processing, provide reasonable assistance to the Customer, taking into account the nature of the Processing, 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; and

(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.

10. **Use of Sub-Processors**

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

10.2 The Company may continue to use those Sub Processors engaged by Company as of the effective date of this DPA, as listed in Annex 3, that can be found in the following link: https://varon.is/subprocessors, subject to Company, in each case as soon as practicable, meeting the obligations set out in this DPA.

10.3 The Company may appoint new Sub-Processors, provided that it provides Customer prior notice (via Company's customers portal) at least 10 days before the appointment takes effect (or earlier if reasonably practical).The Customer may object to such appointment within that notice period by providing written notice only on the grounds of the appointed Sub-Processor's non-compliance with Data Protection Laws. If, in Company's reasonable opinion, such objections are legitimate, the Company shall either refrain from using the proposed Sub-Processor in the context of the processing of Personal Data or shall notify the Customer of its intention to continue using such Sub-Processor. Where the Company notifies the Customer of its intention to continue using the Sub-Processor and does not provide a reasonable alternative, the Customer may terminate the Services in the Main Agreement that require the Processing of Personal Data by such Sub-Processor by written notice to the Company.

10.4 With respect to each Sub-Processor, the Company shall ensure that the arrangement between the 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 Laws, including the requirements of article 28(3) of the GDPR, as applicable.

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

10.6 The 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 is certified under the DPF and complies with its principles with respect to any Personal Data transfers outside the EU, UK or Switzerland, to the US. To the extent the Company Processes Personal Data outside the EEA, the UK or an Approved Jurisdiction and that is not covered by the Company's DPF certification, then the Parties shall be deemed to enter into the Standard Contractual Clauses, subject to the adjustments contained in Exhibit A. In such 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 in the Standard Contractual Clauses).

11.2 The 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), or (iii) in accordance with the DPF principles.

11.3 Annex 3 to this DPA (that can be found in the following link: https://varon.is/subprocessors) 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 The Company will retain Personal Data only for as long as the Main Agreement is in effect or thereafter only to the extent necessary to (a) perform its obligations under the Main Agreement, (b) establish, exercise or defend legal claims or (c) comply with applicable laws or regulations. The Company's retention practices are described in the Company's Privacy Whitepaper at https://www.varonis.com/trust/privacy. Following expiration or termination of the Main Agreement, the Company will delete or return to Customer all Personal Data in its possession or control, unless and to the extent the Company is required by applicable laws to retain any Personal Data. To the extent the Company retains Personal Data after expiration or termination of the Main Agreement, the applicable terms of this DPA will continue to apply to such Personal Data.

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

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

13.2 The Company shall not sell or share such Personal Data (as the terms "sell" and "share" are defined under applicable US Data Protection Laws); and

13.3 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.

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

14. **General**

14.1. Any claim arising out of or in connection with this DPA shall be subject to the terms and conditions of the Main Agreement.

14.2. In the event of a conflict between the Main Agreement (including any document incorporated therein by reference) and this DPA with respect to the subject matter of the DPA, this DPA shall prevail.

14.3. All notices mentioned in this DPA shall be provided by electronic means.

14.4. The Company may change this DPA if the change is required to comply with Data Protection Laws, 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 the Company.

14.5. If the Company intends to amend this DPA and such amendment would have a material adverse impact on Customer (as reasonably determined by Company), the Company will notify the Customer (via the Company's customers portal) at least 10 days before the amendment takes effect, unless a shorter notice period is required to comply with applicable law, regulation, a court order, or guidance issued by a governmental regulator or agency.

14.6. If the Customer processes French health information, Customer should comply with PGSSI, if applicable to it.

Exhibit A – SCC Adjustments

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

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 foregoing, 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 Annex 1 of the DPA, which is incorporated in the Standard Contractual Clauses by reference.

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

   5.1. All information provided under the Standard Contractual Clauses shall apply to the UK Addendum with the necessary changes per the requirement of the UK Addendum.
   5.2. References to "Regulation (EU) 2016/679" or "GDPR" in the Standard Contractual Clauses shall be interpreted as references to the UK GDPR, where applicable
   5.3. References to "EU", "Union" or "Member State" shall be interpreted as references to the United Kingdom, where applicable.
   5.4. References to a "competent supervisory authority" shall be interpreted as references to the UK Information Commissioner's Office.
   5.5. The term "data subjects" shall include data subjects under the UK GDPR.
   5.6. In Clause 17 of the Standard Contractual Clauses, the UK SCCs shall be governed by the laws of England and Wales.
   5.7. n Clause 18(b) of the Standard Contractual Clauses, where the UK SCCs apply, the courts of London, England shall have exclusive jurisdiction.
   5.8. Annexes 1A, 1B and 2 to the UK Addendum shall be replaced with the Annexes attached hereto, respectively.

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

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

6. To the extent the Swiss Federal Act on Data Protection ("FADP") applies, the following shall apply:
   6.1. The Standard Contractual Clauses shall be deemed amended as necessary to comply with the requirements of the Swiss Federal Act on Data Protection of 19 June 1992, as revised (the "FADP"), and the guidance of the Swiss Federal Data Protection and Information Commissioner ("FDPIC").
   6.2. References to "Regulation (EU) 2016/679" or "GDPR" shall be interpreted as references to the FADP, where applicable.
   6.3. References to "EU", "Union" or "Member State" shall be interpreted as references to Switzerland, where applicable.
   6.4. References to a "competent supervisory authority" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner.
   6.5. The term "data subjects" shall include data subjects under the FADP.
   6.6. Clause 17 of the Standard Contractual Clauses shall be governed by the laws of Switzerland.
   6.7. Clause 18(b) of the Standard Contractual Clauses shall designate the competent courts of Switzerland as having jurisdiction.
   6.8. The Standard Contractual Clauses shall also protect data of legal entities, to the extent such protection is required under the FADP.

ANNEX 1 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:

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.

For license(s) or service(s) that may require the Company to process, as part of the Subscriber Data, certain content, then such content will be processed (for example, documents, snippets and prompts).

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 Laws) are intended. Company processes Personal Data provided solely from the Customer and Company does not have control over which Personal Data is processed.

THE FREQUENCY OF THE TRANSFER

Continuous

NATURE OF THE PROCESSING

For the provision of the Services in accordance with the Main Agreement, which may include, depending on the Services, collection, recording, organization or structuring, storage, adaptation or alteration, retrieval, consultation, disclosure, dissemination or otherwise making available, analysis.

PURPOSE OF THE TRANSFER AND FURTHER PROCESSING

As defined in the Main Agreement. The parties may mutually agree in writing to amend this Annex 1.

RETENTION PERIOD

Personal Data will be retained as detailed in this DPA.