Last Updated: June 24, 2024

SecurityScorecard, Inc. Data Processing Addendum

THIS DATA PROCESSING ADDENDUM ("DPA") forms part of and is incorporated into the SecurityScorecard, Inc. ("SSC") End User SaaS Agreement or other written or electronic agreement governing Customer's use of the Service ("**EUSA**") between Customer and SSC (each a "**party**" and together the "**parties")**.

In the course of providing the Service to Customer, SSC may process Customer Data (defined below) and the parties agree to comply with the following provisions with respect to any processing of Customer Data by SSC as a processor or service provider to Customer.

1. **Definitions.** Capitalized terms used in this DPA shall have the meanings given to them in the EUSA unless otherwise defined herein. The following definitions are used in this DPA:

1.1. "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

1.2. "**Authorized Affiliate**" means any Customer Affiliate permitted to use the Service pursuant to the EUSA but have not signed their own EUSA and are not a "Customer" as defined under the EUSA.

1.3. "**CCPA**" means Sections 1798.100 *et seq*. of the California Civil Code and any attendant regulations issued thereunder as may be amended from time to time, including but not limited to the California Privacy Rights Act of 2020 (the "**CPRA**") and its implementing regulations.

1.4. "**Customer Data**" means any Customer Content that is Personal Data and that SSC processes on behalf of Customer in the course of providing the Service, as more particularly described in Schedule A of this DPA.

1.5. "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests (as measured on a fully-diluted basis) then outstanding of the entity in question. The term "Controlled" will be construed accordingly.

1.6. "**Data Protection Laws**" means all data protection and privacy laws regulations applicable to a party and its processing of Personal Data under the EUSA, including, where applicable: (a) the GDPR, (b) all applicable implementations of the GDPR into national law, (c) in respect of the United Kingdom, the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**"), (d) the Swiss Federal Data Protection Act ("**Swiss DPA**"), and (e) the CCPA; in each case, as may be amended, superseded or replaced.

1.7. "**Europe**" means for the purposes of this DPA the European Economic Area ("EEA") and United Kingdom.

1.8. "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

1.9. "**Personal Data**" means any information protected as "personal data", "personal information" or "personally identifiable information" under Data Protection Laws.

1.10. "**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of Customer Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission ("**EEA Restricted Transfer**"); (ii) where the UK GDPR applies, a transfer of Customer Data from the United Kingdom to any other country which is not subject based on adequacy

regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018 ("**UK Restricted Transfer**"); and (iii) where the Swiss DPA applies, a transfer of Customer Data from Switzerland to any other country which is not determined to provide adequate protection for personal data by the Federal Data Protection and Information Commission or Federal Council (as applicable) ("**Swiss Restricted Transfer**").

1.11. "**Standard Contractual Clauses**" means the standard contractual clauses between controllers and processors (Module 2) adopted by European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021 and currently located at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, as amended, superseded or replaced from time to time.

1.12. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data, stored or otherwise processed by SSC in connection with the provision of the Service. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful login attempts, pings, port scans, denial of services attacks, and other network attacks on firewalls or networked systems.

1.13. "**Subprocessor**" means any Processor having access to Customer Data and engaged by SSC to assist in fulfilling its obligations with respect to providing the Service pursuant to the EUSA (excluding any employee, consultant or independent contractor of SSC).

1.14. The terms "**controller**", "**data subject**", "**processor**", "**processing**", "**personal data**" and "**sensitive data**" shall have the meanings given to them in Data Protection Laws or if not defined therein, the GDPR, and the terms "**service provider**", "**business**", "**collects**" (and "**collected**" and "**collection**"), "**consumer**", "**business purpose**", "**sell**" (and "**selling**", "**sale**", and "**sold**"), "**share"** (and "**sharing**" and "**shared**"), and "**service provider**" have the meanings given to them in §1798.140 of the CCPA, as applicable.

1.15. "**UK Addendum**" means the International Data Transfer Addendum (version B1.0) to the EU Commission Standard Contractual Clauses issued by UK Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018, as amended, superseded or replaced from time to time.

2. Roles and Scope of Processing

2.1. **Data Processing Roles.** SSC shall process Customer Data for the Permitted Purpose as a processor on behalf of Customer as the controller. For the purposes of the CCPA (where applicable), SSC shall process Customer Data as a service provider for the Customer as a business.

2.2. **Compliance with Laws.** Each party shall comply with its obligations under Data Protection Laws in respect of any Customer Data it processes under this DPA. For the avoidance of doubt, SSC is not responsible for complying with Data Protection Laws uniquely applicable to Customer by virtue of its business or industry, such as those generally applicable to online service providers.

2.3. **Processing Instructions**. SSC shall process Customer Data in accordance with Customer's documented lawful instructions, unless obligated to do otherwise by applicable law, in which case SSC will notify Customer (unless that law prohibits SSC from doing so on important grounds of public interest). For these purposes, Customer instructs SSC to process Customer Data for the purposes described in Schedule A (the "**Permitted Purpose**", which, where CCPA applies, is a business purpose). The DPA and EUSA are Customer's complete and final instructions. Any additional or alternate instructions must be consistent with the terms of the DPA and the Agreement. Without prejudice to Section 2.4 (Customer Responsibilities), SSC shall promptly notify Customer in writing, unless prohibited from doing so under Data Protection Laws, if it becomes aware or believes that any processing instructions from Customer violates Data Protection Laws (but without obligation to actively monitor Customer's and in such event, SSC shall not be obligated to undertake such processing until such time

as the Customer has updated its processing instructions and SSC has determined that the incidence of non-compliance has been resolved.

2.4. **Customer Responsibilities**. Customer shall, in its use of the Service and provision of instructions, process Customer Data in accordance with Data Protection Laws. Customer is solely responsible for: (i) the accuracy, quality, and legality of the Customer Data, (ii) the means by which Customer acquired such Customer Data; and (iii) the instructions it provides to SSC regarding the processing of such Customer Data. Customer shall ensure (i) that it has provided notice and obtained (or will obtain) all consents and rights necessary for SSC to process Customer Data pursuant to the EUSA and this DPA, (ii) its instructions are lawful and that the processing of Customer Data in accordance with such instructions will not violate applicable Data Protection Laws, and (iii) where the CCPA applies, that the Customer Data is provided to SSC in order to perform the Service for a valid business purpose only.

3. Subprocessing. Customer provides a general prior authorization for SSC to engage Subprocessors and, where CCPA applies, other third party service providers (hereinafter referred to as Subprocessors) in order to provide the Service. The Subprocessors currently engaged by SSC are listed at Schedule B herein. SSC will provide at least ten (10) days' notice to Customer prior to authorizing any new Subprocessor.

4. Security Measures and Security Incident Response

4.1 Security Measures. SSC implements and maintains appropriate and reasonable technical and organizational security measures designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that SSC may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Customer.

4.2 Personnel. SSC restricts its personnel from processing Customer Data without authorization by SSC as set forth in the Security Measures and shall ensure that any person who is authorized by SSC to process Customer Data is under an appropriate obligation of confidentiality.

4.3 Customer Responsibilities. Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data transmitted via the systems it administers and maintains, and taking any appropriate steps to securely encrypt or back up any Customer Data uploaded to the Service.

4.4 Security Incident Response. Upon becoming aware of a Security Incident, SSC will notify Customer without undue delay and, in any case within seventy-two (72) hours after becoming aware. SSC will provide information relating to the Security Incident to Customer promptly as it becomes known or as is reasonably requested by Customer to fulfill Customer's obligations as controller. SSC will also take appropriate and reasonable steps to contain, investigate, and mitigate any Security Incident.

5. Audit and Records.

5.1 Audit Rights. SSC shall make available to Customer all information in SSC's possession or control and provide all assistance in connection with audits of SSC's documentation and policies as Customer may reasonably request, to enable Customer to assess SSC's compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 5 and where applicable, the Standard Contractual Clauses) in accordance with Section 5.2 below.

5.2 Audit Procedures. Where required under Data Protection Laws or where a data protection authority requires, Customer may, on giving at least thirty (30 days) prior written notice, request that Customer's personnel or a third party (at Customer's expense) conduct an audit of SSC's documents and electronic data relating to the processing of Customer Data under the EUSA to the extent necessary to inspect and/or audit SSC's compliance with this DPA,

provided that: (i) Customer shall not exercise this right more than once per calendar year; (ii) such additional audit enquiries shall not unreasonably impact in an adverse manner SSC's regular operations and do not prove to be incompatible with applicable Data Protection Laws or with the instructions of the relevant data protection authority; (iii) before the commencement of such additional audit, the parties shall mutually agree upon the scope, timing, and duration of the audit, and (iv) at all times during the scope of the audit, Customer and any appointed third party will comply with SSC's policies, procedures, and reasonable instructions governing access to its information, including limiting or prohibiting access to confidential information. Without prejudice to the foregoing, SSC will provide all assistance reasonably requested by Customer to accommodate Customer's request.

6. **Data Transfers**. Customer acknowledges and agrees that SSC may transfer and process Customer Data to and in the United States and other locations in which SSC, its Affiliates, or its Subprocessors maintain data processing operations as more particularly described in the Subprocessor list in Schedule B. SSC shall ensure that such transfers are made in compliance with Data Protection Laws and this DPA.

7. **Cooperation** Data Subject and Consumer Rights Requests. SSC shall, taking into account the nature of the processing, reasonably assist Customer in responding to any requests from individuals or applicable data protection authorities relating to the processing of Customer Data for the Permitted Purposes.

   a) In the event that any such request is made to SSC directly, SSC will not respond to such communication directly (except to direct the data subject to contact Customer) without Customer's prior authorization, unless legally compelled to do so. If SSC is required to respond to such a request, SSC will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

   b) If Customer is unable to respond to the request with regard to personal data processed by SSC in its capacity as either a processor or service provider to Customer (as applicable), upon Customer's reasonable request, and subject to any applicable restrictions or exemptions under applicable law, SSC will use reasonable efforts to assist Customer in responding to verified individual requests received by Customer as it relates to the processing of personal data by SSC as a processor or service provider to Customer.

8. **Europe**

   8.1 Scope. The terms in this Section 8 apply only if and to the extent Customer is established in Europe or the Customer Data is otherwise subject to Data Protection Laws applicable to Europe.

   8.2 Subprocessor Obligations. SSC will enter into a written agreement with each Subprocessor imposing data protection obligations no less protective of Customer Data as this DPA or the Data Protection Laws to the extent applicable to the nature of the services provided by such Subprocessor.

   8.3 Subprocessor Objection Right. If Customer objects on reasonable grounds relating to data protection to SSC's use of a new Subprocessor, then Customer shall promptly, provide written notice of such objection to SSC. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties cannot agree to a mutually acceptable resolution, Customer shall as its sole and exclusive remedy have the right to terminate only the relevant affected portion(s) of the service, if any, without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination). Upon termination by Customer pursuant to this Section, SSC shall refund Customer any prepaid fees for the terminated portion(s) of the Service that would have been provided after the effective date of the termination.

   8.4 Transfer Mechanism. To the extent the transfer of Customer Data from Customer to SSC is a Restricted Transfer and Data Protection Laws applicable to Europe require that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be incorporated by reference into and form an integral part of this DPA, as follows:

8.4.1 In connection with an EEA Restricted Transfer: (i) Module Two (*controller to processor transfers*) shall apply and all other modules are deleted; (ii) in Clause 7, the optional docking clause will apply; (ii) in Clause 9 of Module Two, Option 2 will apply and the time period for prior notice of Sub-processor changes is identified in Section 3 of this DPA; (iii) in Clause 11, the optional language will not apply; (iv) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law; (v) in Clause 18(b), disputes shall be resolved before the courts of Ireland; and (vi) Annex I shall be deemed completed with the information set out in Schedule A (Description of Processing/ Transfer) of this DPA.

8.4.2 In connection with a UK Restricted Transfer, the Standard Contractual Clauses shall apply in accordance with Section 8.4.1 above, but as modified and interpreted by the Part 2: Mandatory Clauses of the UK Addendum, which shall be incorporated into and form an integral part of this DPA. Any conflict between the terms of the Standard Contractual Clauses and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Schedule A and Schedule B of this DPA and table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

8.4.3 In connection with a Swiss Restricted Transfer, the Standard Contractual Clauses shall apply in accordance with Section 8.4.1 above, but with the following modifications: (i) any references in the Standard Contractual Clauses to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA and the equivalent articles or sections therein; (ii) any references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; (iii) any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland; and (iv) the Standard Contractual Clauses shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

8.4.4 The rights and obligations afforded by Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

8.5 Data Transfer Arrangements. To the extent SSC adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Data Protection Laws) for the transfer of Personal Data ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Data Protection Laws applicable to Europe and extends to territories to which Personal Data is transferred).

8.6 Notification of Government Access Requests: For the purposes of Clause 15(1)(a) of Standard Contractual Clauses, SSC shall notify Customer and not the data subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the data subject, as necessary.

9. Authorized Affiliates

9.1 Affiliate Communications. Customer is responsible for coordinating all communications with SSC on behalf of its Authorized Affiliates with regard to this DPA. Customer represents that it is authorized to issue instructions as well as make and receive any communications in relation to this DPA on behalf of its Authorized Affiliates.

9.2 Affiliate Enforcement. Authorized Affiliates may enforce the terms of this DPA directly against SSC, subject to the following provisions:

9.2.1 Customer will bring any legal action, suit, claim, or proceeding which the Affiliate would other have it if were a party to the EUSA (each an "Affiliate Claim") directly against SSC on behalf of such Affiliate, except where Data Protection Laws to which the relevant Affiliate is subject require that the Affiliate bring or be a party to such Affiliate Claim; and

9.2.2 for the purpose of any Affiliate Claim brought directly against SSC by Customer on behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by Customer.

10. Limitation of Liability

10.1 To the extent prohibited by applicable law, in no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

10.2 Any claim or remedies Customer or its Affiliates may have against SSC and its respective employees, agents, or Sub-processors arising under or in connection with this DPA including: (i) for breach of this DPA (including the Standard Contractual Clauses or the UK Addendum); (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; (iii) under Data Protection Laws, including but not limited to CCPA, GDPR, UK GDPR or Swiss DPA, including any claims relating to damages paid to a data subject, consumer, or other individual; and (iv) breach of its obligations under the Standard Contractual Clauses or UK Addendum, will, to the maximum extent permitted by law, be subject to any limitation and exclusion of liability provisions (including any agreed aggregate financial cap) that apply under the EUSA.

10.3 For the avoidance of doubt, SSC and its Affiliates' total overall liability for all claims from Customer and its Affiliates arising out of or related to the EUSA and each DPA shall apply in the aggregate for all claims under the EUSA and this DPA together, including by Customer and its Affiliates.

11. CCPA

11.1 Scope. The terms in this Section 11 apply only if and to the extent the Customer Data is subject to Data Protection Laws applicable to the state of California.

11.2 For the purposes of the CCPA, SSC is prohibited from:

(a) selling or sharing Customer Data;

(b) processing Customer Data for targeted and/or cross context behavioral advertising;

(c) retaining, using, or disclosing Customer Data for any purposes other than the specific purposes of performing the Service or as otherwise permitted under the EUSA, this DPA and SSC's Privacy Policy;

(d) retaining using or disclosing Customer Data outside the direct business relationship between SSC and Customer; or

(e) combining Customer Data with any other data if and to the extent doing so would be inconsistent with the Business Purpose or the limitations on service providers under the CCPA or other Data Protection Laws.

11.3 SSC hereby certifies that it understands the restrictions set out in Section 11.2 and will comply with them, and that it will notify Customer if SSC becomes unable to comply with the CCPA.

11.4 Notwithstanding the foregoing and anything to the contrary in the EUSA (including this DPA), Customer acknowledges that SSC shall have a right to process Customer Data for the purposes of creating anonymized, aggregate and/or de-identified information for its own legitimate business purposes.

11.5 SSC maintains, and will continue to maintain during the term of the EUSA, resources for consumers to exercise their rights under the CCPA. If SSC, directly or indirectly, receives a request submitted by a consumer who is an employee of Customer to exercise a right it has under the CCPA in relation to that Consumer's Customer Data, SSC will follow the procedures described in Section 7 of this DPA.

12. General

12.1 The parties agree that this DPA shall replace any existing DPA the parties have previously entered into in connection with the Service.

12.2 As between Customer and SSC, this DPA is incorporated into and subject to the terms of the EUSA and shall be effective and remain in force for the term of the EUSA or the duration of the Service. In the event of any conflict between the terms of this DPA and the terms of the EUSA, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Customer Data.

12.3 Except as described in Section 9 (Authorized Affiliates), in no event shall this DPA benefit or create any right or cause of action on behalf of a third party, but without prejudice to the rights or remedies available to data subjects under Data Protection Laws or this DPA (including the Standard Contractual Clauses).

12.4 Each party acknowledges that the other party may disclose the Standard Contractual Clauses, this DPA, and any privacy related provisions in the EUSA to any regulator or supervisory authority upon request.

12.5 Other than as required by applicable Data Protection Laws or the Standard Contractual Clauses, the dispute mechanisms, including those related to venue and jurisdiction, set forth in the EUSA govern any dispute pertaining to this DPA.

SecurityScorecard

SCHEDULE A

Description of Processing/Transfer

Annex 1(A) List of Parties:

Data Exporter	**Data Importer**
Name: The party named as the 'Customer" in the Order Form or EUSA.	**Name:** SecurityScorecard, Inc. ("SSC")
Address: The address for the Customer associated with its SSC account or as otherwise specified in the Order Form or EUSA. **Contact Person's Name, position and contact details:** Contact Details of Customer **Activities relevant to the transfer:** See Annex 1(B) below. **Signature and Date:** Signature: _____ Title: _____ E-mail: _____ Date: _____	**Address:** 1140 Avenue of the Americas, 19th Floor, New York, NY 10036 **Contact Person's Name, position and contact details:** Owen Denby, General Counsel, privacyteam@securityscorecard.io **Activities relevant to the transfer:** See Annex 1(B) below **Signature and Date:** Signature: _____ Title: General Counsel E-mail: privacyteam@securityscorecard.io Date:
Role: Controller	**Role: Processor**

Annex 1(B) Description of Transfer:

	Description
Categories of Data Subjects:	Depending on the nature of the Service, Personal Data transferred may concern the following categories of data subjects: ● Users of the Service who are Customers' employees, agents, advisors, contractors and other personnel (who are natural persons) ("Customer Personnel') ● Users of the Service who are Customer's vendors' to the extent provided by Customer to SSC.
Categories of Personal Data:	Customer Personnel: The types of Personal Data processed by SSC are determined and controlled by Customer in its sole discretion and may include, but are not limited to the following categories of Personal Data: ● Account log-in credentials such as email, username password, and unique user ● Business contact information including name, email, phone number and job title; ● IP address and user-agent;

Special category data:	SSC does not intentionally collect or process special category data. For purposes of this Agreement, "Special category data" includes but is not limited to the following categories: gender, race or ethnicity, health data, sexual orientation, trade union membership, and any other category of special category.
Frequency of the transfer (one-off or continuous):	Continuous basis for the provision of the Service.
Nature of processing:	The nature of the processing is the performance of the Service in accordance with the EUSA.
Purpose(s) of the data transfer and further processing:	Personal data may be processed for the following purposes: (i) to provide and improve the Service provided to Customer in accordance with the EUSA; (ii) processing initiated by Users in their use of the Service; (iii) to comply with other reasonable instructions provided by Customer (e.g. via email or support tickets) that are consistent with the terms of the EUSA and this DPA, and (iv) to comply with any legal obligation under applicable law, including Data Protection Law.
Retention period (or, if not possible to determine, the criteria used to determine that period):	The duration of the processing is the term of EUSA or any applicable Order Form plus the period from expiration of the EUSA or Order Form (as applicable) until the return or deletion of the personal data by SSC in accordance with the DPA.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	As above.

Annex 1(C): Competent supervisory authority

The competent supervisory authority shall be determined in accordance with Clause 13 of the 2021 Controller-to-Processor Clauses and the GDPR.

SCHEDULE B

SUBPROCESSORS

Company Name	Geographic Location of Entity	Processing Activities Performed by Contractor
Amazon (Amazon Web Services)	US	Hosting and Data Storage
Atlassian (Confluence and Jira)	US	Project management and issue tracking
Datadog	US	Infrastructure Analytics
DocuSign	US	Document signing software
Gong	US	Customer Support
Google	US	Google Workspace (Email, Docs etc.)
Hevo Data	US	Data pipeline platform
Marketo	US	Lead Management, Marketing
Salesforce	US	CRM Platform; Slack for messaging integration
Snowflake	US	Date warehouse
Stripe	US	Payment Processing
Zendesk	US	Customer Support
Zoom	US	Customer Support