Menlo Security

Data Protection Addendum for Customers

This Data Protection Addendum ("**DPA**") is expressly incorporated by reference into the End User License Agreement or other master agreement ("**Agreement**") entered by and between the party identified in the Agreement ("**You**" or "**Customer**") and Menlo Security, Inc. (together with its subsidiaries and Affiliates, "**Menlo Security**" or "**Menlo"**), each a "**Party**" and collectively the "**Parties**," and applies where, and to the extent that Menlo Security Processes Personal Data for Customer when providing Services (as defined below) under the Agreement. For the avoidance of doubt, execution of the Agreement shall constitute Customer's signature and acceptance of this DPA and its Schedules, including Exhibit A and Annex 1 (Standard Contractual Clauses), where applicable.

The Parties agree as follows:

1. **Definitions**. For purposes of this DPA:
   a. "**Affiliate**" means any entity which directly or indirectly controls, is controlled by, or is under common control by a Party. For purposes of the preceding sentence, "control" means direct or indirect ownership or control of fifty-one percent (51%) of the voting interests of the subject entity.

   b. "**Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

   c. "**Data Privacy Laws**" means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* ("**CCPA**"), the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"), the United Kingdom Data Protection Act of 2018 ("**UK Privacy Act**"), and the Swiss Federal Act on Data Protection ("**FADP**"). For the avoidance of doubt, if Menlo Security's Processing activities involving Personal Data are not within the scope of a given Data Privacy Law, such law is not applicable for purposes of this DPA.

   d. "**Data Subject**" means an identified or identifiable natural person about whom Personal Data relates.

   e. "**EU SCCs**" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on 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*, located http://data.europa.eu/eli/dec_impl/2021/914/oj., and completed as set forth in Section 7 below.

   f. "**Personal Data**" includes "personal data," "personal information," "personally identifiable information," and similar terms, and such terms shall have the same meaning as defined by applicable Data Privacy Laws, that is Processed in relation to the Agreement.

   g. "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

   h. **"Processor"** means an entity that processes Personal Data on behalf of a Controller.

   i. "**Representative(s)**" means either Party including its Affiliates, officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

j. "**Security Breach**" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

k. "**Services**" means the Menlo Security services purchased by Customer under the Agreement.

2. **Scope and Purposes of Processing**.

a. Menlo Security will Process Personal Data solely: (1) according to Customer's documented instructions; (2) to fulfill its obligations to Customer under the Agreement, including this DPA; (2) on Customer's behalf; and (3) in compliance with Data Privacy Laws. Menlo Security will not sell Personal Data or otherwise Process Personal Data for any purpose other than for the specific purposes set forth herein. For purposes of this paragraph, "sell" shall have the meaning set forth in the CCPA.

b. Menlo Security will not attempt to link, identify, or otherwise create a relationship between Personal Data and non-Personal Data or any other data without Customer's express authorization.

c. In jurisdictions that distinguish between Controllers and Processors, Menlo Security is the Controller for Personal Data processed to administer and manage the customer relationship. Menlo Security is the Processor for the Personal Data processed by the Services in order to provide its functionality.

3. **Personal Data Processing Requirements**. Menlo Security will:

a. Ensure that the persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

b. Upon Customer's written request, assist Customer in the fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their lawful representatives) for exercising their rights under Data Privacy Laws (such as rights to access or delete Personal Data), at Customer's reasonable expense.

c. Promptly notify Customer of (i) any third-party or Data Subject complaints regarding the Processing of Personal Data; or (ii) any government or Data Subject requests for access to or information about Menlo Security's Processing of Personal Data on Customer's behalf, unless prohibited by Data Privacy Laws. Menlo Security will provide Customer with reasonable cooperation and assistance in relation to any such request. If Menlo Security is prohibited by applicable Data Privacy Laws from disclosing the details of a government request to Customer, Menlo Security shall inform Customer that it can no longer comply with Customer's instructions under this DPA, without providing more details, and await Customer's further instructions. Menlo Security shall use all available legal mechanisms to challenge any demands for data access through national security process that it receives, as well as any non-disclosure provisions attached thereto.

d. Provide reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by applicable Data Privacy Laws, and at Customer's reasonable expense.

e. Provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to Menlo Security under Data Privacy Laws to consult with a regulatory authority in relation to Menlo Security's Processing or

proposed Processing of Personal Data.

4. **Data Security**. Menlo Security will implement appropriate administrative, technical, physical, and organizational measures to protect Personal Data, as set forth in Exhibit B.

5. **Security Breach**. Menlo Security will notify Customer promptly of any known Security Breach and will assist Customer in Customer's compliance with Customer's Security Breach-related obligations, including without limitation, by:

   a. Taking steps to mitigate the effects of the Security Breach and reduce the risk to Data Subjects whose Personal Data was involved; and

   b. Providing Customer with the following information, to the extent known:

      i. The nature of the Security Breach, including, where possible, how the Security Breach occurred, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

      ii. The likely consequences of the Security Breach; and

      iii. Measures taken or proposed to be taken by Menlo Security to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6. **Subprocessors**.

   a. Customer acknowledges and agrees that Menlo Security may use Affiliates and other subprocessors to Process Personal Data in accordance with the provisions within this DPA and Data Privacy Laws. Where Menlo Security sub-contracts any of its rights or obligations concerning Personal Data, including to any Affiliate, Menlo Security will take steps to select and retain subprocessors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with applicable Data Privacy Laws.

   b. Menlo Security's current subprocessors are set forth in Exhibit C (the "**Subprocessor List**"). Customer hereby consents to Menlo Security's use of such subprocessors. Menlo Security will maintain an up-to-date list of its subprocessors, and it will provide Customer with notice (which may be provided through email to Customer's administrator' s email address that was communicated to Menlo Security, or such other reasonable means) of any new subprocessor added to the list. In the event Customer objects to a new subprocessor due to a reasonable belief that the subprocessor cannot provide the level of protection required under this DPA, Menlo Security will use reasonable efforts to make available to Customer a change in the services or recommend a commercially reasonable change to, Customer's use of the services to avoid Processing of Personal Data by the objected-to subprocessor without unreasonably burdening Customer. In the event that Customer objects to a subprocessor as set forth above and Menlo Security is unable to change the services to Customer's reasonable satisfaction, Customer may, in Customer's sole discretion, terminate the applicable part of the Agreement with respect only to those Services which cannot be provided by Menlo Security without the use of the objected to subprocessor by giving written notice to Menlo Security.

7. **Data Transfers and Additional Safeguards**.

   a. Menlo Security will not engage in any cross-border Processing of Personal Data, or transmit, directly or indirectly, any Personal Data to any country outside of the country from which such

Personal Data was collected, without complying with applicable Data Privacy Laws. Where Menlo Security engages in an onward transfer of Personal Data, Menlo Security shall ensure that a lawful data transfer mechanism is in place prior to transferring Personal Data from one country to another.

b. To the extent legally required, by signing this DPA, Customer and Menlo Security are deemed to have signed the EU SCCs, which form part of this DPA and (except as described in Section 7(c) and (d) below) will be deemed completed as follows:

i. Module 2 of the EU SCCs applies to transfers of Personal Data from Customer (as a controller) to Menlo Security (as a processor) and Module 3 of the EU SCCs applies to transfers of Personal Data from Customer (as a processor) to Menlo Security (as a sub-processor);

ii. Clause 7 of Modules 2 and 3 (the optional docking clause) is not included;

iii. Under Clause 9 of Modules 2 and 3 (Use of sub-processors), the Parties select Option 2 (General written authorization). The initial list of sub-processors is set forth in Exhibit C of this DPA and Menlo Security shall propose an update to that list at least 7 days in advance of any intended additions or replacements of sub-processors in accordance with Section 6(b) of this DPA;

iv. Under Clause 11 of Modules 2 and 3 (Redress), the optional language requiring that data subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;

v. Under Clause 17 of Modules 2 and 3 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights). The Parties select the law of Ireland;

vi. Under Clause 18 of Modules 2 and 3 (Choice of forum and jurisdiction), the Parties select the courts of Ireland;

vii. Annex I(A) and I(B) of Modules 2 and 3 (List of Parties) is completed as set forth in Exhibit A of this DPA;

viii. Under Annex I(C) of Modules 2 and 3 (Competent supervisory authority), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission.

ix. Annex II of Modules 2 and 3 (Technical and organizational measures) is completed with Exhibit B of this DPA; and

x. Annex III of Modules 2 and 3 (List of subprocessors) is not applicable as the Parties have chosen General Authorization under Clause 9.

c. With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the effective date at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) ("UK SCCs") forms part of this Addendum and takes precedence over the rest of this Addendum as set forth in the UK SCCs, unless the United Kingdom issues updates to the UK SCCs that, upon notice from Customer, will control. Undefined capitalized terms used

in this provision shall mean the definitions in the UK SCCs. For purposes of the UK SCCs, they shall be deemed completed as follows:

i. Table 1 of the UK SCCs:

1. The Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer.

2. The Key Contact shall be the contacts set forth in the Agreement.

ii. Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties.

iii. Table 3 of the UK SCCs: Annex 1A, 1B, II, and III shall be set forth in Exhibits A, B, and C below.

iv. Table 4 of the UK SCCs: Either Party may end this Addendum as set out in Section 19 of the UK SCCs.

v. By entering into this DPA, the Parties are deemed to be signing the UK SCCs, the Mandatory Clauses in Part 2, and its applicable Tables and Appendix Information.

d. For transfers of Personal Data that are subject to the FADP, the EU SCCs form part of this DPA as set forth in Section 7(b) of this DPA, but with the following differences to the extent required by the FADP: (1) references to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (2) references to personal data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; and (3) the relevant supervisory authority with respect to transfers from Switzerland is the Swiss Federal Data Protection and Information Commissioner.

e. Supplementary Measures. In addition to the obligations under Sections 7(a)-(d), if and to the extent that the Parties will engage in cross-border Processing of Personal Data or will transmit, directly or indirectly, any Personal Data to a country outside of the country from which such Personal Data was collected (including without limitation transfers of Personal Data outside of the EEA, Switzerland or the UK), the Parties agree to the following supplementary measures:

i. All Personal Data shall be encrypted both in transit and at rest using state of the art encryption technology that is robust against the performance of cryptanalysis;

ii. Menlo Security warrants and represents that, as of the date of the Agreement, it has not received any national security data production orders (e.g., pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA Section 702") or U.S. Presidential Policy Directive 28);

iii. Menlo Security will use all reasonable legal mechanisms to challenge any demands for data access through the national security process that Menlo Security receives; and

iv. Menlo Security will provide, up to once per calendar year upon Customer's request, a transparency report indicating the types of binding legal demands for the Personal Data it has received, including national security orders and directives.

8. **Audits**. Menlo Security will make available to Customer all reasonable information necessary to demonstrate compliance with this DPA and will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, provided that, such audit shall occur not more than once every twelve (12) calendar months, upon reasonable prior written notice, and to the extent Menlo Security's personnel are required to cooperate therewith, during Menlo Security's normal business hours.

9. **Return or Destruction of Personal Data**. Except to the extent required otherwise by Data Privacy Laws, Menlo Security will, at Customer's choice and upon Customer's written request, return to Customer and/or securely destroy all Personal Data upon such request or at termination of the Agreement. Except to the extent prohibited by Data Privacy Laws, Menlo Security will inform Customer if it is not able to return or delete the Personal Data.

10. **Survival**. The provisions of this DPA survive the termination or expiration of the Agreement for so long as Menlo Security or its subprocessors Process the Personal Data.

Exhibit A

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s):

Name: The data exporter is Customer.

Activities relevant to the data transferred under these SCCs: The data exporter is a user of the data importer's Services pursuant to their underlying Agreement. The data exporter acts as a controller with respect to its own personal data. To the extent permitted by the Agreement, the exporter also is permitted to use the contracted Services as a processor on behalf of third parties.

Signature and date:

Role: controller

Data importer(s):

Name: Menlo Security

Activities relevant to the data transferred under these SCCs: The data importer is the provider of Services to the data exporter and its customers pursuant to their underlying Agreement. The data importer acts as the data exporter's processor.

Signature and date:

Role: processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred:

The personal data transferred concerns employees, contractors, business partners, representatives and end customers of the data importer and other individuals residing in the European Economic Area, the

United Kingdom and Switzerland, whose personal data is processed by or on behalf of the Customer or Customer's customers and delivered as part of the Services.

Categories of personal data transferred:

The personal data transferred concern the following categories of data (please specify):

Customer's personal data related directly or indirectly to the categories of data subjects listed above, including online and offline support, prospect, and partner data, and Personal Data provided by or on behalf of the Customer or its users of the Services. Such transfer of personal data is determined and controlled by the data exporter in its sole discretion, and may include, and is not limited to the following categories of personal data.

- Any personal data that may be contained in Customer's logs (e.g. user name, user id, IP address, time stamps, websites visited)
- Customer's active directory data
- Any personal data that may be contained in physical binary submitted for analysis
- Any personal data that may be contained in a file submitted for analysis
- Personal data contained in customer logs
- Personal data contained in policy settings
- Company, position
- Login credentials
- Log and usage data
- Device information (device name, device serial number, device type, device owner name, device owner email, timestamp for login)
- IP address
- First and last name, email address, and phone number of Customer's employee(s) appointed to open a support service request
- Browser information, IP address, and other web browsing related protocol information contained in a fille attached to a support ticket
- Personal data contained in a support ticket (Customer controls what it submits)

More detailed categories of personal data are reflected in Menlo Security's Privacy Data Sheet, made available to Customer upon request.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

Unless data exporter or its users use data importer's services to transmit or store sensitive data, data importer does not process sensitive data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous.

Nature of the processing:

Data exporter's Processing activities shall be limited to those discussed in the Agreement and this DPA.

Purpose(s) of the data transfer and further processing:

The objective of the transfer and further processing of personal data by Menlo Security is the access and use of Menlo Security's Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Personal data will be retained for the period of time necessary to provide the Services to Customer under the Agreement, this DPA, and/or in accordance with applicable legal requirements.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Same as above to the extent such information is provided to subprocessors for purposes of providing the Services.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

See Section 7(b)(viii) of this DPA.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Annex 2 to Attachment B, the EU SCCs, is the data security measures located in Exhibit B.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

Data importer shall require its subprocessors to take appropriate technical and organizational measures to provide assistance to the controller and/or data exporter that are no less restrictive than those in Exhibit B.

Exhibit B

MENLO SECURITY DATA SECURITY MEASURES

Menlo Security will implement and maintain the following administrative, technical, physical, and organizational security measures for the Processing of Personal Data:

Menlo Security's Information Security Program includes specific security requirements for its personnel and all subprocessors or agents who have access to Personal Data ("Data Personnel"). Menlo Security's security requirements covers the following areas:

1. Information Security Policies and Standards. Menlo Security will maintain written information security policies, standards and procedures addressing administrative, technical, and physical security controls and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Personal Data.

2. Physical Security. Menlo Security will maintain commercially reasonable security systems at all Menlo Security sites at which an information system that uses or stores Personal Data is located ("Processing Locations") that include reasonably restricting access to such Processing Locations, and implementing measures to detect, prevent, and respond to intrusions.

3. Organizational Security. Menlo Security will maintain information security policies and procedures addressing acceptable data use standards, data classification, and incident response protocols.

4. Network Security. Menlo Security maintains commercially reasonable information security policies and procedures addressing network security.

5. Access Control. Menlo Security agrees that: (1) only authorized Menlo Security staff can grant, modify or revoke access to an information system that Processes Personal Data; and (2) Menlo Security will implement commercially reasonable physical and technical safeguards to create and protect passwords.

6. Virus and Malware Controls. Menlo Security protects Personal Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Personal Data.

7. Personnel. Menlo Security has implemented and maintains a security awareness program to train employees about their security obligations. Data Personnel follow established security policies and procedures. Disciplinary process is applied if Data Personnel fail to adhere to relevant policies and procedures.

8. Business Continuity. Menlo Security implements disaster recovery and business resumption plans that are kept up to date and revised on a regular basis. Menlo Security also adjusts its Information Security Program in light of new laws and circumstances, including as Menlo Security's business and Processing change.

Exhibit C

MENLO SECURITY SUBPROCESSORS

Sub-processor	Personal Data	Location of Data Center	Security Assurances
Amazon Web Services (AWS)	Customer Logs, Policy Settings, Business and Product Analytics	Hosted Globally	As published by Sub-processor here: https://aws.amazon.com/compliance/
Google Cloud Platform (GCP)	Customer Logs, Policy Settings, Business and Product Analytics	Hosted Globally	As published by Sub-processor here: https://cloud.google.com/compliance?hl=en
Sophos	Sandbox Analysis, File Inspection	US, Germany (EU), UK, Japan	InfoSec and Privacy Policies
Salesforce	Account and Registration Information	USA	FedRAMP High/Moderate, GDPR, HIPAA, HITRUST, ISMAP, ISO 27001, 27017, 27018, PCI NSS, SOC2 Type II (and more)
Zendesk	Support Ticket Information	USA	SOC2 Type II, ISO 27001, 27018, FedRAMP LI-SaaS, HIPAA, PCI DSS, Posted policies
Slack	Support Ticket Information	USA	ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC2 Type II, SOC3, APEC for Processors Certification, APEC for Controllers Certification, CSA
Productboard	Support Ticket Information	USA	As published by Sub-processor here: https://www.productboard.com/legal/security-standards/
Grafana	(for non-FedRAMP environments only) Customer Logs, Business and Product Analytics	USA	ISO 27001, SOC2 Type II, PCI DSS, CSA
Marketo	Administrator Contact Information	USA	ISO/IEC 27001
Gainsight	Administrator Contact Information	USA	SOC2 Type II

CDR AND DDR SOLUTIONS SUBPROCESSOR LIST

The following list exclusively applies to Content Disarm and Reconstruction (CDR) and Data Detection and Response (DDR) solutions:

Sub-processor	Personal Data	Location of Data Center	Security Assurances
Amazon Web Services (AWS)	Customer Logs, Policy Settings, Business and Product Analytics	Hosted Globally	As published by Sub-processor here: https://aws.amazon.com/compliance/
Salesforce	Business Operations (Customer Support)	USA	FedRAMP High/Moderate, GDPR, HIPAA, HITRUST, ISMAP, ISO 27001, 27017, 27018, PCI NSS, SOC2 Type II (and more)
Zendesk	Business Operations (Customer Support)	USA	SOC2 Type II, ISO 27001, 27018, FedRAMP LI-SaaS, HIPAA, PCI DSS, Posted policies
Datadog	Customer Analytics	USA	As published by Sub-processor here: https://www.datadoghq.com/security/?tab=compliance
Microsoft (Azure) DevOps	Support Ticket Information	Netherlands	As published by Sub-processor here: https://learn.microsoft.com/en-us/azure/compliance/