Version Date: August 30, 2024

Customer Data Processing Addendum

This Data Processing Addendum, including its Annexes (together, the "**DPA**"), is incorporated into and forms part of the Enterprise License Agreement (also known as the Mobile Endpoint Security License Agreement, Cloud Services Agreement, or master (license) agreement) and all related orders for the Service (defined below) ("**Agreement**") between Lookout, Inc. located at 60 State Street, Suite 1910, Boston, MA 02109 ("**Lookout**") and Customer (as defined below).

This DPA is supplemental to the Agreement and sets out the terms that apply when Personal Data (as defined below) is processed by Lookout under the Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with Data Protection Laws (as defined below) and with due respect for the rights and freedoms of Data Subjects whose Personal Data are processed.

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

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

"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" shall be construed accordingly.

"**Customer**" means the non-Lookout party to the Agreement and this DPA that has access to the Service, or a non-Lookout party that has submitted an order which has been accepted by Lookout and is a party to this DPA.

"**Customer Data**" means the Personal Data which Lookout processes on behalf of Customer as a Data Processor in the course of providing the Service, as more particularly described in this DPA.

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

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

"**Data Protection Laws**" means all international, national, and state data protection and privacy laws and regulations applicable to the processing of Personal Data by Lookout under the Agreement, including: (a) Regulation (EU) 2016/679 (**"GDPR"**); (b) the GDPR as it forms part of UK law by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (collectively, "**UK Data Protection Laws**"); (c) the Swiss Federal Act on Data Protection Act of 2020 and its corresponding ordinances ("**Swiss FADP**"); (d) Directive 2002/58/EC (the "**e-Privacy Directive**"); (e) all applicable national data protection and privacy laws made under or pursuant to (a), (b), (c) or (d); (subsections (a) through (e) shall collectively be known as "**European Data Protection Laws**"); (b) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any implementing regulations ("**CCPA**"), and (c) other applicable U.S. state privacy laws; in each case, as may be amended, superseded, or replaced.

"**Data Privacy Framework**" means (as applicable) the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs operated by the U.S. Department of Commerce, as may be amended, superseded, or replaced.

"**Data Privacy Framework Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as may be amended, superseded, or replaced.

"**Data Subject**" means an identified or identifiable natural person whose rights are protected by Data Protection Laws. "Data Subject" shall also include other variations of the term used in Data Protection Laws, including "Consumer".

"**Europe**" means, for the purposes of this DPA, the member states of the European Economic Area ("**EEA**"), the United Kingdom ("**UK**"), and Switzerland. "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. “Personal Data” shall also include other

variations of the term used in Data Protection Laws, including “Personal Information.”

"**Restricted Transfer**" means a transfer of Personal Data that is subject to European Data Protection Laws to a country outside Europe that does not provide an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws).”

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Service**" means any product or service provided by Lookout to Customer pursuant to the Agreement.

"**Standard Contractual Clauses**" **or** "**SCCs**" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, a copy of which is available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN, as may be amended, superseded, or replaced.

"**Subprocessor**" means any Data Processor engaged by Lookout or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA. Subprocessors may include third parties and Lookout Affiliates but shall exclude any Lookout employees, contractors, or consultants.

"**UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018, as may be amended, superseded, or replaced.

The terms "**supervisory authority**" and "**processing**" shall have the meaning given to them under Data Protection Laws and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

2. Relationship with the Agreement

2.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

2.2 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions of the Agreement, including but not limited to the exclusions and limitations set forth therein. Any claims against Lookout or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall this DPA or any party limit its liability with respect to any Data Subject whose Personal Data is processed under the Agreement.

2.3 Except to the extent required by applicable laws, no one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

2.4 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

2.5 This DPA shall terminate simultaneously and automatically with the termination or expiration of the Agreement.

2.6 Notwithstanding anything to the contrary in the Agreement, in the event of a change in Data Protection Laws or a determination or order by a supervisory authority or competent court affecting this DPA or the lawfulness of any processing activities under this DPA, Lookout may (in its sole discretion) make any amendments to this DPA (or changes to the Service) as are reasonably necessary to ensure continued compliance with Data Protection Laws or any such determination or order.

2.7 Each party acknowledges that the other party may disclose this DPA (including its Annexes and the Standard Contractual Clauses) and any privacy related provisions in the Agreement to a supervisory authority upon request.

3. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that Lookout processes Personal Data that originates from Europe or the United States and/or that is otherwise subject to Data Protection Laws in the course of providing the Service pursuant to the Agreement. The Personal Data that Lookout processes pursuant to the Agreement are described in **Annex 1**. If and to the extent that Lookout processes any Customer Data that is subject to the CCPA, the parties acknowledge that the terms of the CCPA Addendum to this DPA,

which is included in **Annex 4**, shall also apply.

4. Roles and Scope of Processing

4.1 **Role of the Parties**. As between Lookout and Customer, Customer is the Data Controller of Customer Data, and Lookout shall process Customer Data as a Data Processor acting on behalf of Customer.

4.2 **Customer Processing of Customer Data.** Customer agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to Lookout; (ii) it is solely responsible for the accuracy, quality, and lawfulness of Customer Data; and (iii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Lookout to lawfully process Customer Data and provide the Service pursuant to the Agreement and this DPA.

4.3 **Lookout Processing of Customer Data.** Lookout shall process Customer Data only for the purposes described in this DPA and in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to Lookout in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Lookout. Lookout shall inform Customer if it becomes aware that Customer's processing instructions infringe Data Protection Laws.

4.4 **Lookout as a Data Controller**. To the extent that Lookout and/or a Lookout Affiliate processes Personal Data as a Data Controller, Lookout and each Lookout Affiliate shall:

a) comply with Data Protection Laws when processing such Personal Data; and

b) only process such Personal Data to perform its obligations under the Agreement and/or to the extent necessary for the purposes of (i) maintaining and developing Lookout's relationship with Customer (for example, by adding Customer's management contacts to Lookout's CRM database); (ii) billing and invoicing; (iii) compliance with quality control and risk management procedures; (iv) security-related processing (for example, automated scanning for viruses); (v) cybersecurity threat analysis, research, research reporting, and improvement of Lookout's products; (vi) complying with legal and regulatory obligations; and (vii) establishing, exercising and defending legal claims.

5. Subprocessing

5.1 **Authorized Subprocessors**. Customer agrees that Lookout may engage Subprocessors to process Customer Data on Customer's behalf. The Subprocessors currently engaged by Lookout and authorized by Customer are listed in **Annex 3**.

5.2 **Subprocessor Obligations.** Lookout shall (i) enter into a written agreement with each Subprocessor imposing data protection terms that require the Subprocessor to protect Customer Data to an equivalent standard under this DPA; and (ii) remain responsible for any acts or omissions of its Subprocessors that cause Lookout to breach any of its obligations under this DPA.

5.3 **Changes to Subprocessors.** Lookout shall (i) provide an up-to-date list of the Subprocessors it has appointed upon written request from Customer; and (ii) notify Customer (for which email shall suffice) if it appoints any new Subprocessors at least 15 (fifteen) days prior to any such changes. Customer may object in writing to Lookout's appointment of a new Subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Agreement or applicable order for the Service (without prejudice to any fees incurred by Customer prior to suspension or termination). If Customer does not notify Lookout of an objection in accordance with this Section 5.3, Customer shall be deemed to have provided its approval of such appointment. Lookout may appoint a new Subprocessor without giving Customer prior notice if the reason for the appointment is beyond Lookout's reasonable control and, in such instance, Lookout shall notify Customer of the replacement as soon as reasonably practicable and Customer shall retain the right to object to the replacement Subprocessor pursuant to this Section 5.3 above.

6. Security

6.1 **Security Measures**. Lookout shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of Customer Data, in accordance with Lookout's security standards described in **Annex 2** ("**Security Measures**").

6.2 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by

Lookout relating to data security and making an independent determination as to whether the Security Measures meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Lookout 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 purchased by the Customer.

6.3 **Customer Responsibilities**. Notwithstanding the above, 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 when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Service.

7. Security Reports and Audits

7.1 **Security Reports.** Lookout is audited against data protection and information security standards ISO27001 on an annual schedule by independent third-party auditors. Upon request, Lookout shall supply (on a confidential basis) a summary copy of its audit report(s) ("**Report**") to Customer, so that Customer can verify Lookout's compliance with the audit standards against which it has been assessed, and this DPA.

7.2 **Customer's Audit Rights**. Lookout shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm Lookout's compliance with this DPA, provided that Customer shall not exercise this right more than once per year. The parties agree that Customer shall exercise its audit rights under the Standard Contractual Clauses by instructing Lookout to comply with the audit measures described in this Section 7.

7.3 **Lookout Information**. Nothing in this DPA will be construed to require Lookout to provide: (a) trade secrets or any proprietary information; (b) any information that would violate Lookout's confidentiality obligations, contractual obligations, or applicable law; or (c) any information, the disclosure of which could threaten, compromise, or otherwise undermine the security, confidentiality, or integrity of Lookout's infrastructure, networks, systems, or data.

8. International Transfers

8.1 **Data Center Locations**. Lookout may transfer and process Personal Data anywhere in the world where Lookout, its Affiliates or its Subprocessors maintain data processing operations. Lookout shall at all times provide an adequate level of protection for the Personal Data processed, in accordance with the requirements of European Data Protection Laws.

8.2 **Data Privacy Framework**. Lookout complies with the Data Privacy Framework in relation to transfers from Europe to the U.S. The parties acknowledge and agree that Lookout shall use the Data Privacy Framework to lawfully receive Personal Data in the U.S. and Lookout shall ensure that it provides at least the same level of protection to such data as is required by the Data Privacy Framework Principles. Lookout shall notify Customer if it makes a determination that it can no longer comply with its obligations under the Data Privacy Framework.

8.3 **Standard Contractual Clauses.** To the extent that the transfer of Personal Data from Lookout to Customer constitutes a Restricted Transfer, and the Data Privacy Framework does not apply to such transfer (including if the Data Privacy Framework is invalidated), the parties agree that the Standard Contractual Clauses shall be incorporated by reference and apply as follows:

a) **EEA Transfers.** In relation to Personal Data that is subject to the GDPR (i) Lookout shall be deemed the "data importer" and Customer shall be deemed the "data exporter"; (ii) Module One shall apply where Lookout is a Data Controller and Module Two shall apply where Lookout is a Data Processor; (iii) in Clause 7, the optional docking clause shall be deleted; (iv) in Clause 9 of Module Two, Option 2 shall apply and the list of Subprocessors and time period for notice of changes shall be as agreed under Section 5 of the DPA; (v) in Clause 11, the optional language shall be deleted; (vi) in Clause 13, the competent supervisory authority shall be determined in accordance with the GDPR; (vii) in Clause 17, Option 1 shall apply and the SCCs shall be governed by Dutch law; (viii) in Clause 18(b), disputes shall be resolved before the courts of the Netherlands; (ix) Annex I and Annex II shall be deemed completed with the information set out in Annex 1 and Annex 2 of this DPA respectively; and (x) if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA) the SCCs shall prevail to the extent of such conflict.

b) **UK Transfers.** In relation to Personal Data that is subject to UK Data Protection Laws, the SCCs shall apply in accordance with Section 8.3(a) with the following modifications (i) the SCCs shall be modified and interpreted in accordance with the UK Addendum, which shall be deemed incorporated by reference; (ii) Tables 1, 2, and 3 of the UK Addendum shall be deemed completed with the information set out in Annexes 1, 2, and 3 of this DPA; (iii) Table 4 of the UK Addendum shall be deemed completed by selecting “neither party”; and (iv) any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

c) **Swiss Transfers.** In relation to Personal Data that is subject to the Swiss FADP, the SCCs shall apply in accordance with Section 8.3(a) with the following modifications (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP; (ii) references to "EU", "Union" and "Member State law" shall be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" shall be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

8.4 **Alternative Transfer Mechanism.** To the extent that Lookout adopts an alternative data export mechanism for the transfer of Personal Data ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of the mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Laws and extends to the territories to which Customer Data is transferred), and Customer agrees to execute such other and further documents and take such other and further actions as may be reasonably necessary to give legal effect such Alternative Transfer Mechanism.

9. Additional Security

9.1 **Confidentiality of processing**. Lookout shall ensure that any person authorized by Lookout to process Customer Data (including its staff, agents, and contractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

9.2 **Security Incident Response**. Upon becoming aware of a Security Incident, Lookout shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer. Lookout's notification of or response to a Security Incident shall not be construed as an acknowledgment by Lookout of any fault or liability with respect to the Security Incident.

10. Deletion or Return of Data

10.1 Upon termination or expiration of the Agreement, Lookout shall (at Customer's election) anonymize, delete, or return to Customer all Customer Data (including copies) in its possession or control, save that this requirement shall not apply to the extent Lookout is required by applicable law to retain some or all of the Customer Data it has archived on back-up systems, which Customer Data Lookout shall securely isolate and protect from any further processing, except to the extent required by applicable law.

11. Cooperation

11.1 To the extent that Customer is unable to independently access, retrieve, correct, or delete the relevant Customer Data within the Service, Lookout shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from Data Subjects or supervisory authorities relating to the processing of Personal Data under the Agreement. In the event that such requests are made directly to Lookout, Lookout shall not respond to such requests directly without Customer's prior authorization, unless legally compelled to do so. If Lookout is required to respond to such a request, Lookout shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

11.2 If a law enforcement agency sends Lookout a demand for Customer Data, Lookout shall attempt to redirect the law enforcement agency to request such data directly from Customer. As part of this effort, Lookout may provide Customer’s basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Lookout shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Lookout is legally prohibited from doing so.

11.3 To the extent required under Data Protection Laws, Lookout shall (at Customer's expense) provide reasonably requested information regarding Lookout's processing of Customer Data under the Agreement to enable Customer to carry out data protection impact assessments, or similar risk assessments and prior consultations with data protection authorities pursuant to Data Protection Laws.

Annex 1 - Description of the Processing

List of parties

	Data Exporter	**Data Importer**
Name:	The Customer name as set out in the Agreement and/or applicable orders for the Service.	Lookout, Inc.
Address:	The Customer address as set out in the Agreement and/or applicable orders for the Service.	60 State Street, Suite 1910, Boston, MA 02109, United States
Contact Person's Name, position and contact details:	The Customer's contact information as set out in the Agreement and/or applicable orders for the Service.	Lookout, Inc. 60 State Street, Suite 1910, Boston, MA 02109, United States ATTN: Michael Musi, DPO
Activities relevant to the transfer:	Provision of the Service by Lookout to Customer pursuant to the Agreement.	Provision of the Service by Lookout to Customer pursuant to the Agreement.
Role:	Controller	Controller / Processor

Description of the processing

The description of the transfer and processing is set out below, according to the nature of the Service purchased by Customer:

Mobile Endpoint Security (MES)

	Description
Categories of Data Subjects:	Customers' end users, employees, contractors, suppliers and/or other third parties.
Categories of Personal Data:	● Analytics Data, used to analyze product performance on the mobile device ● Application Data, including metadata of all applications installed on a mobile device (including, but not limited to, the names of the apps and the versions of the apps), and in certain circumstances, a copy of the application ● Configuration Data, such as whether a device is configured to allow root access or whether hardware restrictions of the device have been removed ● Device Data, including the device and MDM identifiers of the mobile device ● Firmware/OS Data, including the manufacturer and model of a mobile device, certain technical settings of a mobile device (including the display size of the mobile device and firmware version), the type and version of operating system on a mobile device ● Identification Data, a work email address is optionally collected by the Customer ● Network Data, including metadata about networks which a mobile device connects to (including, but not limited to, the SSID of the network, or the unique MAC/BSSID address of network equipment), and IP address (which can indicate a country and geolocation) ● Web Content Data, including URLs and domains for malicious content and content that requires additional analysis ● Smishing Protection Feature Only: ○ Text Message Data: telephone numbers, timestamps, and message contents of SMS, MMS and RCS (for Android only) messages from unknown senders for Smishing Protection.

	○ Customer Safe Sender List Data: Employees' names, phone numbers, and email addresses stored by Customer used to trigger fraud notifications for text messages sent to Users' devices containing this data.
Sensitive data:	N/A
Frequency:	Continuous
Nature and subject matter:	Lookout and/or its Subprocessors are providing services and support or fulfilling contractual obligations towards Customer, as described in the Agreement. These services may include the processing of Personal Data by Lookout and/or its Subprocessors and performing services on devices that may contain Personal Data.
Purpose(s):	Lookout shall process the data in order to provide the Service, as described under the Agreement.
Duration and retention period:	Lookout shall process the data until it is required to delete or return the data upon termination of the Agreement and in accordance with Section 10 of the DPA.
Lookout's processing role	Data Processor

Security Service Edge (SSE)

	Description
Categories of Data Subjects:	Customers' end users, employees, contractors, suppliers and/or other third parties.
Categories of Personal Data:	● Analytics Data, used to analyze product performance and usage ● Access Data, such as which applications are being accessed, which folders, objects, channels are being accessed within those applications ● Work-related Activity Data, such as attempts to log in or download files from corporate servers ● File Metadata, such as the names, sizes and types of files stored in corporate file sharing services, including who the files are shared with (which may include internal and external email addresses) ● Device Data, including unique device identifiers such as device ID, MDM device IDs, operating system version, browser version and user agent, device compliance posture ● Identification Data, such as work email address, corporate username, corporate user ID and corporate group memberships (e.g. what department an employee is in) ● Network Data, such as the IP address the corporate data was accessed from, the location the user logged in from ● Access or DLP Policy violations, anomalous behaviors or malware access related incident data ● Additional data analyzed on instruction from Customer, such as the content of Customer's files for potential policy violations or malicious code
Sensitive data:	Lookout and/or its Subprocessors do not intentionally collect or process special categories of data (as that term is defined by Data Protection Law) in connection with the provision of the Service under the Agreements. However, Customer or its Affiliates may choose to include this type of data within content that the Customer instructs Lookout to analyze on its behalf. The data that Customer may submit to the Service, including any sensitive data, is determined and controlled by Customer in its sole discretion.
Frequency:	Continuous
Nature and subject matter:	Lookout and/or its Subprocessors are providing services and support or fulfilling contractual obligations towards Customer as described in the Agreement. These services may include the processing of Personal Data by Lookout and/or its Subprocessors and performing services on devices that may contain Personal Data.

Purpose(s):	Lookout shall process the data in order to provide the Service as described under the Agreement. In particular, this includes securing against enterprise data leak and preventing unauthorized access to enterprise resources (applications & data).
Duration and retention period:	Lookout shall process the data until it is required to delete or return the data upon termination of the Agreement and in accordance with Section 10 of the DPA. For Customer data that Lookout analyzes on instruction from Customer, such as the content of Customer's files, Lookout only processes this data for the duration of the scan and does not retain or store the data.
Lookout's processing role	Data Processor

Lookout as Data Controller

	Description
Categories of Data Subjects:	Customers' end users, employees, contractors, suppliers and/or other third parties.
Categories of Personal Data:	The categories of Personal Data described above with respect to Mobile Endpoint Security (MES) and Security Service Edge (SSE). Lookout does not process the content of Customer's files for its own purposes as a Data Controller, except for Text Message Data that potentially contain phishing content, malicious content, and executive fraud content for the Smishing Protection feature.
Sensitive data:	N/A
Frequency:	Continuous
Nature and subject matter:	Lookout processes certain Personal Data for its own legitimate purposes, as described below.
Purpose(s):	Where Lookout is a Data Controller, Lookout shall process the data for its own legitimate business purposes, including for the purposes of (i) maintaining and developing Lookout's relationship with Customer (for example, by adding Customer's management contacts to Lookout's CRM database); (ii) billing and invoicing; (iii) compliance with quality control and risk management procedures; (iv) security-related processing (for example, automated scanning for viruses); (v) cybersecurity threat analysis, research, research reporting, and improvement of Lookout's products; (vi) complying with legal and regulatory obligations; and (vii) establishing, exercising and defending legal claims.
Duration and retention period:	Lookout shall delete the data in accordance with its data retention policies and practices.
Lookout's processing role	Data Controller

Annex 2 – Security Measures

The technical measures in place to protect Customer Data processed by Lookout, Inc. (as updated from time to time in accordance with Section 6.2 of this DPA) are described here:
https://www.lookout.com/documents/legal/securitymeasures.pdf

Annex 3 - List of Subprocessors

Lookout's current Subprocessors engaged to assist in providing the Service are listed here:
https://www.lookout.com/info/subprocessors

Annex 4 - CCPA Addendum

This California Consumer Privacy Act Addendum ("**CCPA Addendum**") is incorporated into the DPA between Lookout and Customer. This CCPA Addendum is supplemental to the DPA and sets out the terms that apply when Customer Data (as defined in the DPA) that is subject to the CCPA is processed by Lookout under the Agreement. The purpose of the CCPA Addendum is to ensure such processing is conducted in accordance with the California Consumer Privacy Act (as amended by the California Privacy Rights Act).

1. **Definitions**.
    a. Any capitalized terms in this CCPA Addendum shall have the meanings set forth in the Agreement or the CCPA. If there is any conflict between the capitalized terms in this Agreement and those in the CCPA, the terms in the CCPA shall prevail.
2. **Scope and Applicability of this CCPA Addendum.**
    a. This CCPA Addendum applies where and only to the extent that Lookout processes Customer Data that is subject to the CCPA in the course of providing the Service pursuant to the Agreement.
3. **Status as Service Provider**. The parties agree that Customer is a Business, and Lookout is its Service Provider in relation to the Customer Data that is processed under the Agreement.
4. **CCPA Disclosures.**
    a. Lookout agrees that it shall only process Customer Data it receives from Customer pursuant to the Agreement for the limited and specified purpose of providing the Service as described under the Agreement and is prohibited from using such Customer Data for any other purpose, except for those permitted under the CCPA.
    b. Lookout shall comply with all applicable provisions of the CCPA, including by providing the same level of protection as required by Customer under the CCPA.
    c. Lookout shall cooperate with Customer in responding to and complying with Consumer requests it receives pursuant to the Agreement that are subject to the CCPA. Customer agrees to provide Lookout with any information it may need to process a Consumer request on its behalf.
    d. Lookout agrees that Customer has the right to take reasonable and appropriate steps to ensure that it processes Customer Data in a manner consistent with Customer's obligations under the CCPA.
    e. Lookout shall notify Customer in the event that it determines that it can no longer meet its obligations under the CCPA.
    f. Lookout agrees that Customer has the right to take reasonable and appropriate steps to stop and remediate Lookout's unauthorized use of Customer Data.
    g. Lookout agrees that, if it subcontracts with another Service Provider or Contractor in relation to providing services to Customer pursuant to the Agreement, Lookout will implement a contract with the Service Provider or Contractor that complies with the CCPA and has the same restrictions on the processing of Personal Information as this Addendum.
    h. Lookout agrees it will not: (i) Sell or Share Customer Data (within the meaning of the CCPA), (ii) retain, use, or disclose Customer Data for any purpose other than for the purposes of providing the Service, or (iii) retain, use, or disclose Customer Data outside of the direct business relationship with Customer or combine Customer Data with Personal Information received from or on behalf of another person or collected from its own interactions with the Consumer, except as permitted under the CCPA.
    i. Lookout certifies that it understands the contractual restrictions in this CCPA Addendum and shall comply with them.