Data Protection Agreement

Addendum to Sales Cookie Terms of Service

Dated 2022-01-03

Introduction

The parties agree that this Sales Cookie Data Protection Addendum ("DPA") sets forth their obligations with respect to the processing and security of Customer Data and Personal Data in connection with Sales Cookie's Services (collectively, the "Services"). The DPA is incorporated by reference into the Sales Cookie's Terms of Service. The parties also agree that, unless a separate written agreement exists, this DPA governs the processing and security of all Customer Data and Personal Data. The provisions of the DPA Terms supersede any conflicting provisions of the Sales Cookie Privacy Policy Statement that otherwise may apply to processing of Customer Data, or Personal Data as defined herein. The provisions of the DPA Terms do not supersede Sales Cookie's Terms of Service.

Applicable DPA Terms and Updates

New Features, Supplements, or Related Capabilities

Notwithstanding the foregoing limits on updates, when Sales Cookie introduces features, supplements or related capabilities that are new (i.e., that were not previously included with a Customer's subscription), Sales Cookie may provide terms or make updates to the DPA that apply to Customer's use of those new features, supplements or capabilities. If those terms include any material adverse changes to the DPA Terms, Sales Cookie will provide Customer a choice to use the new features, supplements, or related software, without loss of existing functionality of the Services. If Customer does not use the new features, supplements, or related software, the corresponding new terms will not apply.

Government Regulation and Requirements

Notwithstanding the foregoing limits on updates, Sales Cookie may modify or terminate the Services in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects Sales Cookie to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for Sales Cookie to continue operating the Services without modification, and/or (3) causes Sales Cookie to believe the DPA Terms or the Services may conflict with any such requirement or obligation.

Electronic Notices

Sales Cookie may provide Customer with information and notices about the Services electronically, including via email, through the Sales Cookie website, or through a website that Sales Cookie identifies. Notice is given as of the date it is made available by Sales Cookie.

Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in the Sales Cookie's Terms of Service. The following defined terms are used in this DPA:

"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Sales Cookie by, or on behalf of, Customer through use of the Services or otherwise obtained or processed by or on behalf of Sales Cookie through a professional services engagement with the Customer.

"Data Protection Requirements" means the GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"Diagnostic Data" means data collected or obtained by Sales Cookie from Customer in connection with the Services. Diagnostic Data may also be referred to as telemetry. Diagnostic Data does not include Customer Data or Service Generated Data.

"DPA Terms" means the terms in the DPA. In the event of any conflict or inconsistency between the DPA and Sales Cookie's Terms of Service, Sales Cookie's Terms of Service shall prevail.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Local EU/EEA Data Protection Laws" means any subordinate legislation and regulation implementing the GDPR.

"GDPR Terms" means the terms regarding processing of Personal Data as per Article 28 of the GDPR.

"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.

"Services" means usage of any aspect of the Site as defined in Sales Cookie's Terms of Service, including any professional services provided by Sales Cookie in relation to the Site.

"Service Generated Data" means data generated or derived by Sales Cookie through the operation of Services. Service Generated Data does not include Customer Data or Diagnostic Data.

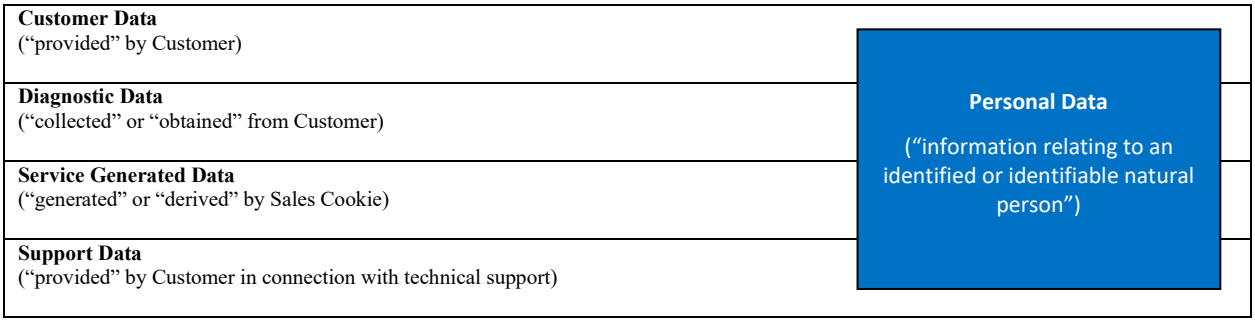
"Standard Contractual Clauses" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010.

"Sub processor" means other processors used by Sales Cookie to process Customer Data and Personal Data, as described in Article 28 of the GDPR.

"Support Data" means all data, including all text, sound, video, image files, or software, that are provided to Sales Cookie by or on behalf of Customer (or that Customer authorizes Sales Cookie to obtain from Services) through Sales Cookie to obtain technical support for Services covered under this agreement. Support Data is a subset of Customer Data.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies. The terms "data importer" and "data exporter" have the meanings given in the Standard Contractual Clauses.

For clarity, and as detailed above, data defined as Customer Data, Diagnostic Data, and Service Generated Data may contain Personal Data. For illustrative purposes, please see the chart inserted below:



Above is a visual representation of the data types defined in the DPA. All Personal Data is processed as a part of one of the other data types (all of which also include non-personal data). The DPA Terms focus on Customer Data and Personal Data.

General Terms

Compliance with Laws

Sales Cookie will comply with all laws and regulations applicable to its provision of the Services, including security breach notification law and data protection requirements. However, Sales Cookie is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to SaaS service providers. Sales Cookie does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third-party regarding Customer's use of Services, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Data Protection Terms

This section of the DPA includes the following subsections:

- Scope
- Nature of Data Processing; Ownership
- Disclosure of Processed Data
- Processing of Personal Data; GDPR
- Data Security
- Security Incident Notification
- Data Transfers and Location
- Data Retention and Deletion
- Processor Confidentiality Commitment
- Notice and Controls on Use of Sub processors
- California Consumer Privacy Act (CCPA) Terms
- Biometric Data
- Limitation of Liability
- How to Contact Sales Cookie
- Appendix A – Security Measures

Scope

The DPA Terms apply to all Sales Cookie Services.

Nature of Data Processing; Ownership

Sales Cookie will use and otherwise process Customer Data and Personal Data only (a) to provide Customer the Services in accordance with Customer's documented instructions, and (b) for Sales Cookie's legitimate business operations incident to delivery of the Services to Customer, each as detailed and limited below. As between the parties, Customer retains all right, title and interest in and to Customer Data. Sales Cookie acquires no rights to Customer Data, other than the rights Customer grants to Sales Cookie in this section. This paragraph does not affect Sales Cookie's rights over software or services Sales Cookie licenses to Customer.

Processing to Provide Customer the Services

For purposes of this DPA, "to provide" Services consists of:

Delivering functional capabilities (calculating and managing commissions);

Troubleshooting issues (monitoring, detecting, and repairing errors); and

Ongoing improvement (installing updates, improving software).

When providing Services, Sales Cookie will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.

Processing for Sales Cookie's Legitimate Business Operations

For purposes of this DPA, "Sales Cookie's legitimate business operations" consist of the following, each as incident to delivery of the Services to Customer: (1) billing and account management; (2) commission management (e.g., configuring and calculating incentive compensation including commissions and bonuses for internal and external payees); (3) reporting and business modeling (e.g., incentive compensation planning, management and administration); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Sales Cookie's Services; (5) improving accessibility or security of the Services; and (6) and compliance with accounting and legal obligations (subject to the limitations on disclosure of Processed Data outlined below).

When processing for Sales Cookie's legitimate business operations, Sales Cookie will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section.

Disclosure of Processed Data

Sales Cookie will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Personal Data; and (c) any other data processed by Sales Cookie in connection with the Services that is Customer's confidential information under the Sales Cookie Terms. All processing of Processed Data is subject to Sales Cookie's obligation of confidentiality under the Sales Cookie Terms.

Sales Cookie will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Sales Cookie with a demand for Processed Data, Sales Cookie will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or

provide access to any Processed Data to law enforcement, Sales Cookie will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Sales Cookie will promptly notify Customer unless prohibited by law. Sales Cookie will reject the request unless required by law to comply. If the request is valid, Sales Cookie will attempt to redirect the third party to request the data directly from Customer.

Sales Cookie will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Sales Cookie is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Sales Cookie may provide Customer's basic contact information to the third party.

Processing of Personal Data; GDPR

All Personal Data processed by Sales Cookie in connection with the Services is obtained as either Customer Data, Diagnostic Data, or Service Generated Data. Personal Data provided to Sales Cookie by, or on behalf of, Customer through use of the Services is also Customer Data. Pseudonymized identifiers may be included in Diagnostic Data or Service Generated Data and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from other data is also Personal Data.

To the extent Sales Cookie is a processor or sub processor of Personal Data subject to the GDPR, the GDPR Terms govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and Sales Cookie agree that Customer is the controller of Personal Data and Sales Cookie is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case Sales Cookie is a sub processor; or (b) as stated otherwise in the Services Terms or this DPA. When Sales Cookie acts as the processor or Sub processor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that Sales Cookie Services (including the DPA Terms and any applicable updates), along with the product documentation and Customer's use and configuration of features in the Services, are Customer's complete documented instructions to Sales Cookie for the processing of Personal Data. Information on Sales Cookie's Terms of Service can be found at https://salescookie.com/Home/Terms or a successor location. Any additional or alternate instructions must be agreed to according to the Customer specific agreement with Sales Cookie. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Sales Cookie that Customer's instructions, including appointment of Sales Cookie as a processor or sub processor, have been authorized by the relevant controller.

To the extent Sales Cookie uses or otherwise processes Personal Data subject to the GDPR for Sales Cookie's legitimate business operations incident to delivery of the Services to Customer, Sales Cookie will comply with the obligations of an independent data controller under GDPR for such use. Sales Cookie is accepting the added responsibilities of a data "controller" for processing in connection with its legitimate business operations to: (a) act consistent with regulatory requirements, to the extent required under GDPR; and (b) provide increased transparency to Customers and confirm Sales Cookie's accountability for such processing. Sales Cookie employs safeguards to protect Customer Data and Personal Data in processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR.

Processing Details

The parties acknowledge and agree that:

Subject Matter. The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled "Nature of Data Processing; Ownership" above and the GDPR.

Duration of the Processing. The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.

Nature and Purpose of the Processing. The nature and purpose of the processing shall be to provide the Services pursuant to Sales Cookie's Terms of Service and for Sales Cookie's legitimate business operations incident to delivery of the Services to Customer (as further described in the section of this DPA entitled "Nature of Data Processing; Ownership" above).

Categories of Data. The types of Personal Data processed by Sales Cookie when providing the Services include: (i) Personal Data that Customer elects to include in Customer Data; and (ii) those expressly identified in Article 4 of the GDPR that may be contained in Diagnostic Data or Service Generated Data. The types of Personal Data that Customer elects to include in Customer Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in The Standard Contractual Clauses (Processors) of the DPA.

Data Subjects. The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in The Standard Contractual Clauses (Processors) of the DPA.

Data Subject Rights; Assistance with Requests

Sales Cookie will make available to Customer, in a manner consistent with the functionality of the Services and Sales Cookie's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Sales Cookie receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with Services for which Sales Cookie is a data processor or Sub processor, Sales Cookie will redirect

the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services. Sales Cookie shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires Sales Cookie to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Sales Cookie and keep it accurate and up to date. Sales Cookie may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Sales Cookie will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Sales Cookie Security Policy. Sales Cookie will make that policy available to Customer, along with descriptions of the security controls in place for the Services and other information reasonably requested by Customer regarding Sales Cookie security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. Services implement and maintain security measures set forth in Appendix A for the protection of Customer Data.

Data Encryption

Customer Data (including any Personal Data therein) in transit over public networks between Customer and Sales Cookie, or between Sales Cookie data centers, is encrypted by default. Sales Cookie also encrypts Customer Data stored at rest in Services.

Data Access

Sales Cookie employs least privilege access mechanisms to control access to Customer Data (including any Personal Data therein). For Services, Sales Cookie maintains Access Control mechanisms described in the table entitled "Security Measures" in Appendix A – Notices, and there is no standing access by Sales Cookie personnel to Customer Data. Role-based access controls are employed to ensure that access to Customer Data required for service operations is for an appropriate purpose, for a limited time, and approved with management oversight.

Customer Responsibilities

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for Services meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Sales Cookie provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls.

Auditing Compliance

Sales Cookie will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows:

Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.

Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

Each audit will be performed by qualified security auditors at Sales Cookie's selection and expense.

Each audit will result in the generation of an audit report ("Sales Cookie Audit Report"), which Sales Cookie will make available upon request. The Sales Cookie Audit Report will be Sales Cookie's Confidential Information and will clearly disclose any material findings by the auditor. Sales Cookie will promptly remediate issues raised in any Sales Cookie Audit Report to the satisfaction of the auditor. If Customer requests, Sales Cookie will provide Customer with each Sales Cookie Audit Report. The Sales Cookie Audit Report will be subject to non-disclosure and distribution limitations of Sales Cookie and the auditor.

To the extent Customer's audit requirements under the Standard Contractual Clauses or Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Sales Cookie makes generally available to its customers, Sales Cookie will promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and Sales Cookie will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Sales Cookie to unreasonably delay performance of the audit. To the extent needed to perform the audit, Sales Cookie will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data and Personal Data by Sales Cookie, its Affiliates, and its Sub processors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Sales Cookie, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Sales Cookie's other customers or to Sales Cookie systems or facilities not involved in the Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Sales Cookie expends for any such audit, in addition to the rates for services performed by Sales Cookie. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Sales Cookie and Sales Cookie shall promptly cure any material non-compliance.

Nothing in this section of the DPA varies or modifies the standard Sales Cookie's Terms of Service or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Requirements.

Security Incident Notification

If Sales Cookie becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by Sales Cookie (each a "Security Incident"), Sales Cookie will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Sales Cookie selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Services portal. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Sales Cookie shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Sales Cookie's notification of or response to a Security Incident under this section is not an acknowledgement by Sales Cookie of any fault or liability with respect to the Security Incident.

Customer must notify Sales Cookie promptly about any possible misuse of its accounts or authentication credentials or any security incident related to Services.

Data Transfers and Location

Data Transfers

Customer Data and Personal Data that Sales Cookie processes on Customer's behalf may not be transferred to, or stored and processed in a geographic location except in accordance with the DPA Terms and the safeguards provided below in this section. Taking into account such safeguards, Customer appoints Sales Cookie to transfer Customer Data and Personal Data to the United States or any other country in which Sales Cookie or its Sub processors operate and to store and process Customer Data and Personal Data to provide the Services, except as described elsewhere in the DPA Terms.

Sales Cookie will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, Sales Cookie complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail, although Sales Cookie does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18. Sales Cookie agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

Location of Customer Data at Rest

For the Services, Sales Cookie will store Customer Data at rest within the United States only. Sales Cookie does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

Data Retention and Deletion

At all times during the term of Customer's subscription, Customer will have the ability to access, extract and delete Customer Data stored in Sales Cookie.

Except for free trials and free subscription services, Sales Cookie will retain Customer Data that remains stored in a limited function account for 30 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 30-day retention period ends, Sales Cookie will disable Customer's account and delete the Customer Data and Personal Data, unless Sales Cookie is permitted or required by applicable law, or authorized under this DPA, to retain such data.

The Services may not support retention or extraction of software provided by Customer. Sales Cookie has no liability for the deletion of Customer Data or Personal Data as described in this section.

Processor Confidentiality Commitment

Sales Cookie will ensure that its personnel engaged in the processing of Customer Data and Personal Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Sales Cookie shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Customer Data and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on use of Sub processors

Sales Cookie may hire sub processors to provide certain limited or ancillary services on its behalf. Customer consents to this engagement and to Sales Cookie Affiliates as sub processors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Sales Cookie of the processing of Customer Data and Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Sales Cookie is responsible for its sub processors' compliance with Sales Cookie's obligations in this DPA. Sales Cookie makes available information about sub processors on a Sales Cookie website. When engaging any sub processor, Sales Cookie will ensure via a written contract that the Sub processor may access and use Customer Data or Personal Data only to deliver the services Sales Cookie has retained them to provide and is prohibited from using Customer Data or Personal Data for any other purpose. Sales Cookie will ensure that sub processors are bound by written agreements that require them to provide at least the level of data protection required of Sales Cookie by the DPA, including the limitations on disclosure of Processed Data. Sales Cookie agrees to oversee the Sub processors to ensure that these contractual obligations are met.

From time to time, Sales Cookie may engage new sub processors. Sales Cookie will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new sub processor at least 30 days in advance of providing that sub processor with access to Customer Data. Additionally, Sales Cookie will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new sub processor at least 30 days in advance of providing that sub processor with access to Personal Data other than that which is contained in Customer Data. If Sales Cookie engages a new sub processor for new Services, Sales Cookie will give Customer notice prior to availability of that Services.

If Customer does not approve of a new sub processor, then Customer may terminate any subscription for the affected Services without penalty by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Sales Cookie to re-evaluate any such new sub processor based on the applicable concerns. If the affected Services is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Sales Cookie will remove payment obligations for any subscriptions for the terminated Services from subsequent invoices to the Customer.

California Consumer Privacy Act (CCPA)

If Sales Cookie is processing Personal Data within the scope of the CCPA, Sales Cookie makes the following additional commitments to Customer. Sales Cookie will process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any "sale" exemption. In no event will Sales Cookie sell any such data. These CCPA terms do not limit or reduce any data protection commitments Sales Cookie makes to Customer in the DPA Terms, Sales Cookie Terms, or other agreement between Sales Cookie and Customer.

Biometric Data

If Customer uses Services to process Biometric Data, Customer is responsible for: (i) providing notice to data subjects, including with respect to retention periods and destruction; (ii) obtaining consent from data subjects; and (iii) deleting the Biometric Data, all as appropriate and required under applicable Data Protection Requirements. Sales Cookie will process that Biometric Data following Customer's documented instructions (as described in the "Processor and Controller Roles and Responsibilities" section above) and protect that Biometric Data in accordance with the data security and protection terms under this DPA. For purposes of this section, "Biometric Data" will have the meaning set forth in Article 4 of the GDPR and, if applicable, equivalent terms in other Data Protection Requirements.

Limitation of Liability

The limitations of liability in the Sales Cookie's Terms of Service apply.

How to Contact Sales Cookie

If Customer believes that Sales Cookie is not adhering to its privacy or security commitments, Customer may contact Sales Cookie's Data Protection Officer at privacy@salescookie.com. Sales Cookie's mailing address is:

Sales Cookie

1100 106th Ave

Ste 903

Bellevue, Washington 98004 USA

Appendix A – Security Measures

Sales Cookie has implemented and will maintain for Customer Data in the Services the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms), are Sales Cookie's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership**. Sales Cookie has appointed a security officer responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. Sales Cookie personnel with access to Customer Data are subject to confidentiality obligations. **Risk Management Program**. Sales Cookie performed a risk assessment before launching the Services and processing Customer Data. Sales Cookie retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Handling** - Sales Cookie classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - Sales Cookie imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. Sales Cookie personnel must obtain Sales Cookie authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Sales Cookie's facilities.
Human Resources Security	**Security Training**. Sales Cookie informs its personnel about relevant security procedures and their respective roles. Sales Cookie also informs its personnel of possible consequences of breaching the security rules and procedures. Sales Cookie will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. Sales Cookie limits access to facilities where information systems that process Customer Data are located to identified authorized individuals. **Protection from Disruptions**. Sales Cookie uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. Sales Cookie uses industry standard processes to delete Customer Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Sales Cookie maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** - Sales Cookie utilizes Microsoft Azure's data recovery procedures for all data stored in the Azure cloud. - Sales Cookie has specific procedures in place governing access to copies of Customer Data. - Sales Cookie reviews data recovery procedures every twelve months. - Sales Cookie logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Sales Cookie has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries** - Sales Cookie encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. **Event Logging**. Sales Cookie logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Sales Cookie maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** - Sales Cookie maintains and updates a record of personnel authorized to access Sales Cookie systems that contain Customer Data. - Sales Cookie deactivates authentication credentials that have not been used for a period not to exceed six months. - Sales Cookie identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Sales Cookie ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed. - Sales Cookie restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Sales Cookie instructs Sales Cookie personnel to disable administrative sessions when leaving premises Sales Cookie controls or when computers are otherwise left unattended. - Sales Cookie stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Sales Cookie uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Sales Cookie requires that the passwords be renewed regularly. - Where authentication mechanisms are based on passwords, Sales Cookie requires the password to be at least eight characters long. - Sales Cookie ensures that de-activated or expired identifiers are not granted to other individuals. - Sales Cookie monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password.

Domain	Practices
	- Sales Cookie maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Sales Cookie uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Sales Cookie has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - Sales Cookie maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Sales Cookie (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Sales Cookie tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Sales Cookie security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Sales Cookie utilizes Microsoft Azure's emergency and contingency plans for the Customer Data stored in the Azure cloud. - Sales Cookie utilizes Microsoft Azure's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.