Secure Privacy Service

Customer has requested “Secure Privacy SAAS Services” (the “Secure Privacy Services” under the Agreement) to TravelClick. The Secure Privacy Services are governed by separate terms and conditions below (the “Secure Privacy Pass-Thru Terms of Use”). To the extent the Secure Privacy Pass-Thru Terms of Use conflict with any provision in the Agreement, the Secure Privacy Pass-Thru Terms of Use govern your access to and use of the Secure Privacy Services and your relationship with such third-party provider.

Customer will pay for all fees related to the Secure Privacy Service in accordance with Exhibit A attached hereto and Section 2 (Fees) of the Agreement. Customer understands and agrees that the Secure Privacy Service is based on the number of domains set forth on Exhibit A and any request for additional domains after execution of the Agreement will incur additional fees.

Secure Privacy Pass-Thru Terms of Use

These Pass-Thru Terms of Use apply to the use of Secure Privacy SAAS Services made available to End Users according to the contract between Secure Privacy and TravelClick via the applicable login link and other web pages designated by Secure Privacy.

These Pass-Thru Terms of Use constitute a binding contract on you and govern your use of and access to the SAAS Services by you as an End User or your employees in connection with the SAAS Services.

By accepting these Pass-Thru Terms of Use, You agree to be bound by the Pass-Thru Terms of Use when using the SAAS Services. If You are entering into this Agreement on behalf of a company, organization or another legal entity (an “Entity”), You are agreeing to this Agreement for that Entity and representing to Secure Privacy that You have the authority to bind such Entity and its Affiliates to this Agreement, in which case the terms “End User” “You,” “Your” or a related capitalized term herein shall refer to such Entity and its Affiliates. If You do not have such authority, or if You do not agree with this Agreement, You must not accept this Agreement and may not use the SAAS Services.

1. Definitions

The following terms have the following meanings:

Account means any accounts or instances created for an End User within the SAAS Services.

Agreement means the Pass-Thru Terms of Use for the SAAS Services.

Applicable Data Protection Law means all applicable laws and regulations relating to the Processing of Personal Data and privacy, including the EU’s General Data Protection Regulation (2016/679/EC), and all laws and regulations implementing or made under them and any amendment or re-enactment of them.

Confidential Information means all information disclosed by Secure Privacy to You, or by You to Secure Privacy, which is in tangible form and labeled “confidential” (or with a similar label) or which a reasonable person would understand to be confidential given the nature of the information and circumstances of disclosure, including, but not limited to, information relating to Secure Privacy’s security policies and procedures. For the purposes of this Agreement, all Service Data shall be deemed Confidential Information. Notwithstanding the foregoing, Confidential Information shall not include information that (a) was already known to the receiving Party at the time of disclosure by the disclosing Party; (b) was or is obtained by the receiving Party from a third party not under an obligation of confidentiality with respect to such information; (c) is or becomes generally available to the public other than by violation of this Agreement or another valid agreement between the Parties; or (d) was or is independently developed by the receiving Party without the use of the disclosing Party’s Confidential Information.

Consulting Services means consulting and professional services (including any training, development or implementation services) provided by Secure Privacy or its subcontractors as indicated in an Order Form or statement of work independent of this Agreement.

Domain means a unique domain or subdomain that will be added to the Account and granted access to the SAAS Services.

End-User means any person given access to the SAAS Services by Secure Privacy according to this Agreement.

Personal Data means any information relating to an identified or identifiable natural person ("Data Subject"); 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;

Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data by Secure Privacy, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. *Personnel* means employees and/or non-employee service providers and contractors of Secure Privacy engaged by the Secure Privacy in connection with performance hereunder.

SAAS Service(s) means the products and services that are provided to You by Secure Privacy, via the applicable login link and other web pages designated by Secure Privacy.

Service Data means Your data stored in the SAAS Services

Subprocessor means any Data Processor engaged by Secure Privacy in the Processing of Personal Data.

Subscription Term means the period for which you are provided with the SAAS Services by Secure Privacy.

Third-Party Services means third-party products, applications, services, software, networks, plugins, systems, directories, websites, databases and information obtained separately by You pursuant to an agreement with a third-party.

2. General Conditions; Access to and use of the services

2.1. During the Subscription Term and subject to compliance by You with this Agreement, You have the limited right to access and use the SAAS Services. We will (a) make the SAAS Services available to You pursuant to this Agreement; (b) use commercially reasonable efforts to make the SAAS Services available 24 hours a day, 7 days a week, except (i) during planned downtime for upgrades and maintenance of the SAAS Services (of which We will use commercially reasonable efforts to notify You in advance both through Our Site and updates to which You can subscribe ("Planned Downtime"); and (ii) for any unavailability caused by circumstances beyond Our reasonable control, including, for example, an act of God, act of government, flood, fire, earthquake, civil unrest, act of terror, strike or other labor problem (other than one involving Our employees), Internet service provider failure or delay, Third-Party Services, or acts undertaken by third parties, including without limitation, denial of service attack ("Force Majeure Event"). Secure Privacy reserves the right to monitor and periodically audit Your use of the SAAS Services to ensure that Your use complies with the Agreement. For clarity, Secure Privacy will not provide standard customer support for the SAAS Services to You.

2.2. A high-speed Internet connection is required for proper transmission of the SAAS Services. You are responsible for procuring and maintaining the network connections that connect Your network to the SAAS Services, including, but not limited to, "browser" software that supports protocols used by Secure Privacy, including the Transport Layer Security (TLS) protocol or other protocols accepted by Secure Privacy, and to follow procedures for accessing services that support such protocols. We are not responsible for notifying

You of any upgrades, fixes or enhancements to any such software or for any compromise of data, including Service Data, transmitted across computer networks or telecommunications facilities (including but not limited to the Internet) which are not owned, operated or controlled by Secure Privacy. We assume no responsibility for the reliability or performance of any connections as described in this section.

2.3. In addition to complying with the other terms, conditions and restrictions set forth below in this Agreement, You agree not to (a) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share or otherwise commercially exploit or make the SAAS Services available to any third party except in furtherance of Your internal business purposes as expressly permitted by this Agreement; ; (b) modify, adapt, reverse engineer or hack the SAAS Services or otherwise attempt to gain unauthorized access to the SAAS Services or related systems or networks; (c) falsely imply any sponsorship or corporate affiliation with Secure Privacy, (d) use the SAAS Services other than in the manner provided by Secure Privacy, resulting in a violation of applicable law, including but not limited to, violation of any person's privacy rights; (e) use the SAAS Services to store or transmit files, materials, data, text, audio, video, images or other content that infringes third party's intellectual property rights; (f) use the SAAS Services in any manner that interferes with or disrupts the integrity or performance of the SAAS Services and its components; (g) attempt to decipher, decompile, reverse engineer or otherwise discover the source code of any Software making up the SAAS Services; (h) use the SAAS Services to knowingly post transmit, upload, link to, send or store any viruses, malware, trojan horses, time bombs, or any other similar harmful software ("Malicious Software"); (i) use or launch any automated system that accesses the SAAS Services (e.g. bot) in a manner that sends more request messages to a SAAS Service server in a given period of time than a human can reasonably produce in the same period by using a conventional on-line web browser; or (j) use the SAAS Services in violation of this Agreement.

2.4. In addition to Our rights as set forth herein, We reserve the right, in Our reasonable discretion, to temporarily suspend Your access to and use of a Service if We detect any Malicious Software connected to the Account or Domain or to the use of the SAAS Services by You.

2.5. You may not access the SAAS Services if You are a direct competitor of Secure Privacy, except with Secure Privacy's prior written consent. You may not access the SAAS Services for the purposes of monitoring performance, availability, functionality, or for any benchmarking or competitive purposes.

2.6. You acknowledge that Secure Privacy may update the features and functionality of the SAAS Services during the Subscription Term.

3. Confidentiality; Security and Privacy

3.1. Subject to the express permissions set forth in this Agreement, each Party will protect each other's Confidential Information from unauthorized use, access or disclosure in the same manner as it protects its own Confidential Information, but no less than with reasonable care. Except as otherwise expressly permitted pursuant to this Agreement, each of us may use each other's Confidential Information solely to exercise our respective rights and perform our respective obligations under this Agreement and shall disclose such Confidential Information (a) solely to the Personnel who have a need to know such Confidential Information for such purposes and who are bound to maintain the confidentiality of, and not misuse, such Confidential Information; (b) as necessary to comply with an order or subpoena of any administrative agency or court of competent jurisdiction; or (c) as reasonably necessary to comply with any applicable law or regulation.

3.2. Secure Privacy will maintain reasonable administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of Service Data. Those safeguards will include, but will not be limited to, measures for preventing access, use, modification or disclosure of the Service Data by the Personnel except (a) to provide the SAAS Services and prevent or address service, support or technical problems; (b) for compliance with this Agreement or applicable law; or (c) as You expressly permit in writing.

3.3. To the extent Service Data constitutes Personal Data, You and Secure Privacy hereby agree that You shall be deemed to be the data controller and the relevant entity in Secure Privacy shall be deemed to be the data processor as those terms are understood under the Applicable Data Protection Law and the Data Processing Agreement between Secure Privacy and End User (see Attachment 1). Service Data may be hosted by Secure Privacy or their respective authorized third-party service providers in the EU, the US or other locations around the world.

3.4. You agree that Secure Privacy and its agents, including Subprocessors shall have the right to access the Account and to use, modify, reproduce, distribute, display and disclose Service Data to the extent necessary to provide the SAAS Services, including, without limitation, in response to Your support requests. Any third-party service providers utilized by the Secure Privacy will only be given access to the Account and Service Data as is reasonably necessary to provide the Services and will be subject to confidentiality obligations that are commercially reasonable and substantially consistent with the standards described.

3.5. You acknowledge that Secure Privacy uses essential cookies for the SAAS Services to function. Currently, Secure Privacy uses the following types of cookies:

1. s_e_c_u_r_e_k_e_y – to enable the system to record the opt-in or opt-out of cookie consent inside the system account.
2. ss-id cookies – temporary cookies for getting information during your session on the websites on how you use them. These cookies last only until the end of your session on the websites. They get deleted when you leave the websites.
3. ss-pid – persistent cookies for getting information during your session on the websites on how you use them. These cookies stay on your computer after the end of your session and use the collected data to improve your experience when you return to the websites.

4. Intellectual Property Rights

Each Party shall retain all rights, title, and interest in and to all its respective patents, inventions, copyrights, trademarks, domain names, trade secrets, know-how, and any other intellectual property and/or proprietary rights (collectively, “Intellectual Property Rights”). The rights granted to You to use the Service(s) under this Agreement do not convey any additional rights in the Service(s) or in any Intellectual Property Rights associated therewith. Subject only to limited rights to access and use the Service(s) as expressly stated herein, all rights, title and interest in and to the SAAS Services and all hardware, Software and other components of or used to provide the SAAS Services, including all related Intellectual Property Rights, will remain with Secure Privacy and belong exclusively to Secure Privacy. Secure Privacy shall have a free, worldwide, transferable, sub-licensable (through multiple layers), assignable, irrevocable and perpetual license to implement, use, modify, commercially exploit, and/or incorporate into the SAAS Services or otherwise use any suggestions, enhancement requests, recommendations or other feedback We receive from You or other third parties acting on Your behalf.

5. Third-Party Services

Your access and use of Third Party Services Providers to integrate with Secure Privacy are governed solely by the terms and conditions of such Third Party Service Providers, and We do not endorse, are not responsible or liable for, and make no representations as to any aspect of such Third Party Service Providers, including, without limitation, their content or the manner in which they handle, protect, manage or Process data (including Service Data) or any interaction between You and the provider of such Third Party Service Service Providers. We cannot guarantee the continued availability of such Third Party Service Providers’ features, and may cease enabling access to them without entitling You to any refund, credit, or Third Party Service Provider compensation, if, for example, and without limitation, the Third Party Service Provider ceases to make their services available for interoperation with the Secure Privacy Service in a manner acceptable to Secure Privacy. You irrevocably waive any claim against Secure Privacy with respect to such Third Party Service Provider. We are not liable for any damage or loss caused or alleged to be caused by or in connection with Your enablement, access or use of any such Third Party Service Provider, or Your reliance on the privacy practices, data security processes or other policies of such Third Party Service Provider.

6. Cancellation and Termination

6.1. Secure Privacy or You may elect to terminate the Account upon thirty (30) days' prior written notice to Secure Privacy such termination to be effective on the last day of the then current term of Your agreement with TravelClick.

6.2. We reserve the right to modify, suspend or terminate the SAAS Services (or any part thereof), the Account or Your rights to access and use the SAAS Services at any time if We believe that You have violated this Agreement and You do not cure the violation within 30 days of Our notification to You.

6.3. Upon termination of the contract, you may export the data within the system at no charge. You may also request the data to be handed over to You by Secure Privacy for a fee.

7. Representations, Warranties, and Disclaimers

7.1. Each Party represents that it has voluntarily and validly entered into this Agreement and has the legal power to do so.

7.2. Except as specifically set forth herein, the SAAS Services, including all server and network components, are provided on an "as is" and "as available" basis, without any warranties of any kind, express or implied, to the fullest extent permitted by law, and we expressly disclaim any and all warranties, whether express or implied, including, but not limited to, any implied warranties of merchantability, title, fitness for a particular purpose, and non-infringement. you acknowledge that we do not warrant that the SAAS Services will be uninterrupted, timely, secure, error-free or free from viruses or other Malicious Software, and no information or advice obtained by you from us or through the SAAS Services shall create any warranty not expressly stated in this agreement.

8. Limitation of Liability

8.1. Under no circumstances and under no legal theory (whether in contract, tort, negligence or otherwise) shall we, or our affiliates, officers, directors, employees, agents, service providers, suppliers or licensors , nor TravelClick, be liable to you or any third party for any lost profits, lost sales or business, lost data, business interruption, loss of goodwill, or for any type of indirect, incidental, special, exemplary, consequential or punitive loss or damages, or any other loss or damages incurred by you or any third party in connection with this Agreement, the SAAS Services or Consulting Services, regardless of whether we have been advised of the possibility of or could have foreseen such damages.

8.2. Notwithstanding anything to the contrary in this agreement, Secure Privacy's aggregate liability to you or any third party arising out of this Agreement or otherwise in connection with any subscription to, or use or employment of the SAAS Services, shall in no event exceed the then-current annual fee for the SAAS Services found at https:\\secureprivacy.ai\pricing.

8.3. Secure Privacy provides a tool for collecting and managing user consent on websites. This tool is provided 'as is' and without warranty of any kind, express or implied. You understand that compliance with Applicable Data Protection Law and other national and international data protection laws is a multifaceted matter, which is reflected in all processes and areas of operation of your business, not only on your website. Moreover, a user consent management mechanism on a website alone does not guarantee full compliance of the website with Applicable Data Protection Law and other national and international data protection laws. Therefore, Secure Privacy does not guarantee and is not liable for the compliance of your website and/or your business and data processing activities, for which user consent is collected, with Applicable Data Protection Law and other national and international data protection laws, and it is your sole responsibility to ensure such compliance. -

8.4. Any claims or damages that You may have against Secure Privacy shall only be enforceable against Secure Privacy and not any other entity or its officers, directors, representatives or partners.

Attachment 1: Data Processing Addendum

Definitions

"Personal Data" means any information relating to an identified or identifiable natural person **("Data Subject")**; 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.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Data Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the controller;

"Data Protection Legislation" means all applicable laws and regulations relating to the Processing of Personal Data and privacy, including the EU's General Data Protection Regulation (2016/679/EC), and all laws and regulations implementing or made under them and any amendment or re-enactment of them.

"Data Processing Subcontractor" means any Data Processor engaged by Secure Privacy in the Processing of Personal Data.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Personal Data Processing

The provision of the Secure Privacy services (the “Services”) involve the Processing of Personal Data by Secure Privacy on behalf of the End User. The provisions of this Addendum govern the Processing of Personal Data by Secure Privacy for all services provided under this Agreement.

The Parties agree that for any Personal Data Processed as a result of or pursuant to this Agreement, Secure Privacy shall be the Data Processor and shall Process Personal Data on behalf of the End User and shall not do anything which may put the End User in breach of applicable Data Protection Legislation. Secure Privacy shall:

1) only Process Personal Data exclusively for the performance of the Services and in accordance with the written instructions of the End User from time to time and in any case in accordance with the terms of the Agreement and this DPA, except to the extent that any law to which Secure Privacy is subject prevents Secure Privacy from complying with such instructions or requires the Processing of Personal Data other than as instructed by the End User. In such a case Secure Privacy shall inform the End User of the legal requirements before Processing, unless that law prohibits such information on important grounds of public interest. Secure Privacy must immediately inform the End User if, in its opinion, an instruction infringes Data Protection Legislation. Secure Privacy must ensure that any natural person acting under the authority of Secure Privacy who has access to Personal Data does not act outside the instructions.
2) procure that access to Personal Data is limited to those members of its personnel and data processing subcontractors who need access to Personal Data to meet Secure Privacy’s obligations under the Agreement and this DPA and in the case of any access by any personnel, such part or parts of the Personal Data as is strictly necessary for the performance of the duties of the personnel. Secure Privacy shall ensure that all personnel: (i) are informed of the confidential nature of Personal Data; (ii) have undertaken training relating to the handling of Personal Data; and (ii) are aware of both the Secure Privacy duties and their personal duties and obligations under Data Protection Legislation and the Agreement and the DPA.
3) take reasonable steps to ensure the reliability of any members of personnel that have access to the Personal Data.
4) ensure that any Personal Data is subject to appropriate technical and organisational measures against unauthorised or unlawful Processing of the Personal Data and against accidental loss or destruction of, or damage to, the Personal Data in accordance with any applicable Data Protection Legislation and take all measures required under Article 32 of the GDPR to ensure a level of security appropriate to the risks of varying likelihood and severity to the rights and freedoms of natural persons. The obligation involves Secure Privacy making a risk assessment and then implementing measures to address the identified risks.
5) cease to use the services of a Data Processing Subcontractor if the End User has reasonably objected to the subcontracting in writing; where a Data Processing Subcontractor is engaged, the Secure Privacy shall impose the Personal Data Processing obligations set out in this DPA on such Data Processing Subcontractor, and the Data Processing Subcontractor will perform the Services in accordance with the provisions of the Agreement, this DPA and applicable Data Protection Legislation; Secure Privacy shall remain fully liable for the performance of the Data Processing Subcontractors obligations. Secure Privacy shall provide evidence of the contractual terms between the Secure Privacy and any Data Processing Subcontractor to End User upon request; state the precise location where the Personal Data being processed under the Agreement and the DPA are stored, see Annex B. Secure Privacy must update the information to reflect any changes.

6) not transfer any Personal Data including to locations outside the European Economic Area against the provisions of the Data Protection Legislation.

7) maintain up-to-date records of processing activities related to the End User's Personal Data in accordance with the requirements of the GDPR. The End User may at any time request a copy of these records and Secure Privacy is under an obligation to hand over such records without undue delay.

8) Inform the End User immediately of any requests or queries from a Data Subject, regulatory authority or any other law enforcement authority regarding Processing of Personal Data under the Agreement and provide the End User with any information and assistance that may reasonably be required to respond to any such requests of queries.

9) provide reasonable assistance to the End User, in accordance with and as set forth in applicable Data Protection Legislation, in respect of the End User's compliance with (i) the security of the Processing; (ii) the notification of a Personal Data Breach to the competent supervisory authority; (iii) the communication of the Personal Data Breach to the Data Subject; (iv) the carrying out of an assessment of the impact of the envisaged Processing operations on the protection of Personal Data; and (v) prior consultations to the competent supervisory authority, taking into account the nature of the Processing undertaken by Secure Privacy and the information available to Secure Privacy. Furthermore, Secure Privacy must assist the End User in complying with any obligations resting upon the End User under applicable law in force from time to time where Secure Privacy's assistance is implied or where Secure Privacy's assistance is necessary for the End User's compliance with their obligations.

10) at the choice of End User, delete or return all Personal Data to End User after the end of the provision of the Services relating to processing unless Secure Privacy is required to retain the Personal Data by applicable Law;

11) If Secure Privacy has become aware of a potential or actual Personal Data Breach, Secure Privacy must immediately notify End User in writing. This notification must as a minimum include information about the nature of the Personal Data Breach identified and, if possible, the categories of persons (Data Subjects) affected as well as the number of data subjects affected, the categories of Personal Data concerned and the number of Personal Data records concerned as well as the mitigating measures taken or suggested by Secure Privacy in respect of the Personal Data Breach identified.

12) Secure Privacy must immediately notify the End User in case of any failure by Secure Privacy as well as any Data Processing Subcontractor to comply with their Personal Data Processing obligations and must take action to rectify the non-compliance as soon as possible. If such rectification is not possible, Secure Privacy must propose mitigating measures.

13) maintain complete and accurate records and information related to End User's Personal Data to demonstrate its compliance with this DPA and make available to the End User information reasonably necessary to demonstrate compliance with Secure Privacy 's Personal Data Processing obligations under the Agreement and the DPA including but not limited to certifications of security measures in place and allow for audits by End User or End User's designated auditor. The engagement of a mutually agreed upon third-party auditor to conduct the audit on behalf of the End User shall be subject to an executed written confidentiality agreement between the third-party auditor and Secure Privacy. The End User may use the audit reports only for the purposes of meeting its regulatory audit requirements and / or confirming compliance with the requirements of this DPA. The audit reports shall constitute confidential information of the parties under the terms of the Agreement. This right to audit may

be exercised but not more than once a year and on a prior 90 days-notice, Secure Privacy may refuse the proposed date and time of audit and propose multiple new reasonable dates and times that fall within 90 days after the notice. End User may once per calendar year, demand documentation of Secure Privacy's continuous assessment of its authorised Processing Subcontractors. End User may at any time request Secure Privacy to forward its authorised Data Processing Subcontractors' documentation of the effectiveness of security measures, documentation of Personal Data Breaches, processing records, auditors' statements as well as any other information, documentation and material which End User could require from Secure Privacy.

ANNEX A

INSTRUCTIONS

This Annex A forms an integral part of the Data Processing Addendum.

Subject-matter of Processing/instructions

The End User hereby instructs Secure Privacy to Process Personal Data for the purpose of provision of Services under this Agreement. The SAAS Service is a service whereby End Users ask Secure Privacy to host a cookie/plugin consent management solution on End Users' websites.

Purpose of Processing

Personal Data must be Processed on behalf of the End Users in accordance with the purpose stated in the Data Processing Addendum. Secure Privacy may not use the Personal Data for any other purpose. The Personal Data may be Processed only on instructions from End User.

Processing of Personal Data

Nature of processing

Secure Privacy's Processing of Personal Data primarily concerns the following:

Secure Privacy makes its cookie consent solution available to End Users who add/configure/remove End-users to the administration panel. The End Users get access, configure the solution and install it on their website to make it operational.

Categories of data subjects

Domain visitors and Domain administrators.

Categories of Personal Data

The following types of Personal Data are being processed: Email address, IP address, Name of contact person.

Return/Erasure of Personal Data

Secure Privacy will erase all Personal Data being Processed on behalf of the End User as well as any copies thereof 60 days after the termination of the account and will erase Personal Data upon request.

Location(s) for Processing

The locations for Secure Privacy's Processing are described in Annex B.

Transfers to Third Countries and International Organisations

Secure Privacy may not transfer Personal Data to Third Countries or International Organisations, unless permitted under the Agreement and the DPA.

ANNEX B

INFORMATION ABOUT DATA PROCESSING SUBCONTRACTORS AND CONTACT POINT

This Annex B forms an integral part of the Data Processing Addendum between the End User and Secure Privacy concerning this Agreement.

In connection with the provision of the Processing Services under the Agreement, the processing of Personal Data will take place at the below locations. Approval is obtained by the End User’s signature to a new Annex B, which will replace previously signed annexes.

Data Processing Subcontractors

Secure Privacy works with Data Processing Subcontractors to provide specific functionalities within the SAAS Services. The Data Processing Subcontractors are available at https://secureprivacy.ai/subprocessors. In order to provide the relevant functionality these Data Processing Subcontractors access Personal Data. Their use is limited to the indicated Services and purposes.

The End Users specifically authorised the use of the above Data Processing Subcontractors for the processing. Secure Privacy may not – without the End User’s specific and written authorisation – use the individual Data Processing Subcontractors for any “other” Processing than agreed or have the described Processing be carried out by another Data Processing Subcontractor.

Infrastructure Data Processing Subcontractors:

Entity name	**Entity type**	**Entity country**
Microsoft Azure	Cloud Service Provider	Netherlands

The security measures implemented by Microsoft Azure and used by Secure Privacy data center include, but are not limited to data encryption, malware protection, background checks, penetration testing, intrusion detection, and audits. The rest of the measures are listed in the Microsoft Azure Security Documentation available on https://docs.microsoft.com/en-us/azure/security/.

Contact points:

The Parties can contact each other via the below contact points. The Parties must keep each other up to date on changes to the contact points.

Service Provider’s contact point	
Email	legal@secureprivacy.ai

End User’s contact point	
Email	