HOXHUNT SAAS END USER LICENSE AGREEMENT

Hoxhunt is a cybersecurity company providing human risk management platform as a corporate Software as a Service solution. This Hoxhunt SaaS End User License Agreement (the "Agreement") is entered into by Hoxhunt and the legal entity listed below using the Services provided through the Reseller (the "Customer"), each a "Party" and together the "Parties", as of the date the Agreement is signed by both Parties (the "Effective Date"). The Agreement is governed by the Hoxhunt Terms of Service attached hereto.

The relevant Hoxhunt legal entity acting as the contracting party in the Agreement is defined based on the Customer's location. Therefore, "Hoxhunt" or "Service Provider" in the Agreement shall mean either: (i) Hoxhunt Inc. (61-2044575), if the Customer's address specified below is in the United States or Canada; (ii) Hoxhunt GmbH (HRB 105923 Amtsgericht Düsseldorf), if the Customer's address specified below is in Germany; or (iii) Hoxhunt Oy (2758722-7), if the Customer's address specified below is in any other location than as specified in (i) or (ii) above, or if no address of the Customer is specified .

Contact Information:	
Customer: New Mexico Department of Health Address: 1190 S SAINT FRANCIS DR, Santa Fe, New Mexico 87505, US Employer identification number (EIN):	Contact: Emilia Mack, emilia.mack@doh.nm.gov
Service Provider: Hoxhunt	Contact: paige.kahle@hoxhunt.com Contact for topics related to the Agreement: Hoxhunt Legal legal@hoxhunt.com

Services, Service Term and **Service Fees** shall be specified in a separate agreement entered into by the Reseller and the Customer regarding the sale and purchase of the Services, and which shall be flowed down to the Service Provider in an order entered into by the Reseller and the Service Provider, where applicable.

IN WITNESS WHEREOF, the Parties hereto have duly executed the Agreement as of the Effective Date.

Hoxhunt	New Mexico Department of Health
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Hoxhunt Specification

The Service Provider's Human Risk Management Platform is available in three different platform tiers called *Professional*, *Enterprise* and *Unlimited*. All platform tiers include self-service tools for user management, phishing simulation, and security awareness training content management as well as tools for reporting. Otherwise, each tier contains a specific set of platform features as described below. Functionality offering has been assigned into three separate purpose-oriented modules called *Comply*, *Change* and *Respond*. For companies with less than 500 employees there is also a separate *SMB* module that is designed for smaller companies.

Human Risk Management Platform (applicable as ordered by the Customer)

Human Risk Management Platform Professional consists of basic features included in the Service Provider's core platform, such as the Hoxhunt reporter plugin and self-service knowledge base. Comply, Change and SMB modules are available for Human Risk Management Platform Professional.

Human Risk Management Platform Enterprise contains all features of Human Risk Management Platform Professional and advanced features such as the Hoxhunt onboarding and customer success services, as well as the Hoxhunt API connections when available. Comply, Change and Respond modules are available for Human Risk Management Platform Enterprise.

Human Risk Management Platform Unlimited includes all features of Human Risk Management Platform Enterprise as well as all other existing Service Provider's core platform features, such as the Hoxhunt data pipeline and custom branding. Comply, Change and Respond modules are available for Human Risk Management Platform Unlimited.

Modules (applicable as ordered by the Customer)

Comply — With Advanced Security Awareness Training and Threat Feed functionality, the Customer can create training packages from a set of training modules and assign, grade, and measure the completion. Additionally, standardized

phishing email campaigns can be scheduled and sent to establish a risk baseline for email-based threats. Threat Feed functionality collects all of the user-reported threats into a single view for easy navigation and safe inspection.

Change — With Adaptive Phishing Training, Intelligent Threat Feed functionality and Instant Feedback feature, personalized phishing emails are scheduled and sent automatically, and they get more difficult the better the Users are. Users reporting a threat can instantly receive feedback about what they should do with the email they deemed suspicious. Based on the content of the email, the Service Provider can show threat indicators, which are concrete reasons explaining why the email may be malicious. Additionally, Intelligent Threat Feed functionality includes automatic maliciousness classification for all items in the threat feed.

Respond — With Feedback Rules and Incident Orchestration features, the Customer can set up rules to identify safe emails and simulated phishing attacks from third parties. Feedback Rules feature prevents the submission of false positive reports and provides customized feedback to the reporter. Additionally, the user-reported spam and phishing emails are prioritized to an admin's attention based on pre-set triggers, and the number of incidents that the admin needs to handle are decreased by filtering out threats which do not match the pre-set criteria. Further, Incident Orchestration feature eases analyzing reported emails by clustering the emails belonging to the same attack or legitimate campaign under one incident.

SMB (only available for companies with less than 500 employees) — With Advanced Security Awareness Training, Adaptive Phishing Training, and Threat Feed functionality, personalized phishing emails are scheduled and sent automatically, and they get more difficult the better the Users are. The Customer can create training packages from a set of training modules and assign, grade, and measure the completion. Threat Feed functionality collects all of the user-reported threats into a single view for easy navigation and safe inspection.

Customer Support

Customer Success — With Human Risk Management Platform Enterprise and Unlimited, the Customer shall receive periodic communication with the Service Provider's customer success representative to reflect upon progress, feedback, and areas of development. In addition, the Customer may contact the Service Provider's customer support if they have any question, feedback, or need help with the Services through the platform or e-mail at support@hoxhunt.com.

Onboarding Support — The Service Provider shall provide all necessary customer support in order to launch the Services within the Customer's email environment (defined as either one Microsoft Outlook application tenant or one Google Gmail application tenant). The Parties shall use their best efforts to launch the Services on the start date specified in the Order. Unless otherwise agreed in writing, onboarding of additional email environments is billable at USD 3,000 per environment.

Launch — The Customer is required to fulfill any reasonable responsibilities which may be designated by the Service Provider in order to facilitate the launch of the Services. These reasonable responsibilities of the Customer can include, among other things, providing access to relevant systems to the Service Provider, whitelisting of IP addresses from which simulation threats are sent, enabling the Service Provider plugin, and provision of User data. Delays to the launch of the Services flowing from the Customer's failure to fulfil its reasonable responsibilities shall not excuse the Customer from payment of the Service Fees nor incur any liability on behalf of the Service Provider.

HOXHUNT TERMS OF SERVICE

To agree on the terms and conditions applicable to the Hoxhunt solution, the Customer must enter into a binding agreement regarding the delivery of the Services, either directly with the relevant Hoxhunt legal entity or through an authorized third-party partner. Unless otherwise agreed in writing, these Hoxhunt Terms of Service (the "Terms") apply to all Services provided by Hoxhunt to the Customer, whether the Agreement with the Customer is entered into by Hoxhunt or the Partner.

1. Definitions

In the Agreement, the following terms have the meanings set forth below:

"Additional Users"	means the active Users in excess of the number of Users included in the fixed yearly Service Fees as specified in the Order or as agreed between the Partner and the Customer;
"Affiliate"	means any legal entity that: (i) directly or indirectly owns or controls a Party; (ii) is under the same direct or indirect ownership or control as a Party; or (iii) is directly or indirectly controlled by a Party, in each case where "control" means ownership of more than fifty percent (50%) of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of such entity;
"Agreement"	means, in case the delivery of the Services is agreed between the Customer and the Service Provider, the Order and these Terms together, or in case the delivery of the Services is agreed between the Customer and the Partner, these Terms;
"AI Features"	is defined in Clause 2.2.6;
"AI Input"	is defined in Clause 2.2.6;
"AI Output"	is defined in Clause 2.2.6;
"Beta Services"	means beta or other early-stage services provided by the Service Provider which are optional for the Customer to use and not generally available;
"Confidential Information"	means all non-public information disclosed by the disclosing Party to the receiving Party in any form or medium, whether written, oral or electronic, that is marked as confidential or that the receiving Party should reasonably understand to be confidential in nature from the circumstances of disclosure or the nature of the information. The Confidential Information includes, but is not limited to, the terms of any agreement, including this Agreement, and the discussions, negotiations and proposals related thereto, and information concerning the disclosing Party's products and services, business and operations including, but not limited to, information relating to business plans, financial records, customers, suppliers, vendors, products, product samples, costs, sources, strategies, inventions, procedures, sales aids or literature, technical advice or knowledge, contractual agreements, pricing, product specifications, trade secrets, procedures, distribution methods, inventories, marketing strategies and interests, algorithms, data, designs, drawings, work sheets, blueprints, concepts, samples, inventions, manufacturing processes, computer programs and systems and know-how or other Intellectual Property Rights of the disclosing Party and its Affiliates, and the Service Provider Properties. However, material or information that is (i) commonly available or otherwise public without the receiving Party having broken confidentiality obligations, or (ii) which the Party has legally obtained from a third party without a confidentiality obligation; or (iii) which was in the possession of the receiving Party prior to receiving it from the other Party; or (iv) which the Party has independently developed without utilizing any material or information received from the other Party as established by competent documentary evidence; or (v) which the Party is obligated to disclose due to laws, regulations, or orders from either authorities or courts, is not considered Confidential Information. Although the Personal Data is also Confidential Information, the terms of the DPA shall always prevail in respect of the processing of Personal Data;
"Customer"	means a legal entity end-customer using the Services, whether the Agreement with the Customer regarding the Services is entered into directly by the Service Provider or through a Partner;
"Customer Data"	means all data and information collected, processed or stored as a result of the Customer's or its Users' use of the Services;
"DPA"	is defined in Clause 4;
"Documentation"	means the then-current technical and non-technical specifications for the Services contained in the system, specification, support and configuration documentation, which are made generally available by the Service Provider to its customers or otherwise provided to the Customer;
"Environment of Use"	is defined in Clause 2.1.4;
"Feedback"	means all comments, feedback, development ideas, inventions or other opinions provided by the Customer or its Users to the Service Provider;

“Intellectual Property Rights”	means any and all intellectual property rights, such as patents, inventions, rights in designs, rights in know-how, trademarks, database rights, trade secrets, domain names, techniques, methods and copyrights (including without limitation right to amend and further develop as well assign one’s rights), in each case whether registered or not, whether registrable or not, and including applications for grant of any of the foregoing and all rights or forms of protection having equivalent or similar effect to any of the foregoing which may now or at any time hereafter exist anywhere in the world;
“Internal Business Purposes”	means use of the Services in the course of the Customer’s typical internal operations;
“Order”	means a document according to which the Services are ordered by the Customer, such as (i) the Service Provider’s offer accepted in writing (by manual signature, email confirmation or otherwise electronically) by the Customer, or (ii) the Customer’s order accepted by the Service Provider in writing (by manual signature, email confirmation or otherwise electronically);
“Partner”	means an authorized third-party partner who resells the Services to the Customer;
“Party”	means the Service Provider or the Customer, collectively referred to as the “Parties”;
“Services”	means the information, documents and services the Service Provider provides to the Customer under the Agreement;
“Service Credit”	is defined in Clause 9.1;
“Service Fees”	means any fees payable by the Customer, or otherwise due to the Service Provider or due to the Partner;
“Service Provider Properties”	is defined in Clause 5.1;
“Service Term”	means the twelve (12)-month period of time (unless otherwise agreed in the Order or between the Partner and the Customer, if relevant) during which the Service Provider provides the Services to the Customer, unless terminated by either Party in accordance with Clause 10 of these Terms;
“Terms”	means these Hoxhunt Terms of Service;
“Third-Party Applications”	is defined in Clause 2.2.5;
“Third-Party Claim”	is defined in Clause 6.1; and
“Users”	means those certain employees, agents, and contractors of the Customer and its Affiliates who are authorized by the Customer to use the Services in accordance with the Agreement.

2. Rights, Restrictions and Responsibilities

2.1 Of the Customer —

2.1.1 Right to Use — Subject to the ongoing compliance with the Agreement by the Customer and its Users, in consideration for the Service Fees, the Service Provider grants to the Customer and its relevant Affiliates a limited, non-exclusive, non-transferable, non-sublicensable, and revocable right to access and use the Services during the Service Term within the limitations as set forth in the Agreement, solely for the Customer’s Internal Business Purposes and in accordance with the Documentation and the Agreement. The Service Provider and its licensors reserve all rights not expressly granted in the Agreement.

2.1.2 Per User Basis — The Users may access the Services on a “one-User-per-license” basis. Each license can only be used by one (1) User at any one time. The Customer shall have sole liability and responsibility for the acts and omissions of its Users (including any use of the Services that has taken place using the usernames and passwords of its Users), including, without limitation, the Users’ compliance with the Documentation and the Agreement. The Customer shall immediately inform the Service Provider of any unauthorize access to the Services, including if any third parties gain knowledge of a username or password, or of any suspected misuse of a username or password of its User.

2.1.3 Usage Restrictions — The Customer shall not sell, rent out, lend, transfer, or otherwise make available the right of access and use of the Services to any third parties without express prior written consent from the Service Provider. The Customer shall not copy, save, reproduce, transfer, distribute, sell, disclose, or otherwise make public the contents of the Services or any part thereof. The Customer shall not repair, open, disassemble, decompile, reverse engineer or otherwise modify any part of the Services.

2.1.4 Environment of Use — The Customer is solely responsible at its own cost for acquiring and maintaining its Environment of Use and the protection of its Environment of Use. For purposes of the Agreement, ”Environment of Use” means all the Customer’s hardware and software devices and infrastructures situated downstream from the demarcation point of the Service Provider’s network and which are used by the Customer to facilitate use of the Services.

2.1.5 Obtain Rights — The Customer is required to obtain and maintain all Customer- or Users-related licenses, consents, rights of use, and permissions necessary for the Service Provider to perform its obligations under the Agreement for the Customer, including, for example, a valid license for an email application into which to integrate the Service Provider’s reporter plugin and all necessary consents from the Users in relation to providing the Service Provider’s training to such Users.

2.2 Of the Service Provider —

2.2.1 Right to Develop — The Service Provider has the right to develop and change the Services, its availability and the system requirements for the equipment and Environment of Use needed to use the Services, provided that there is no material degradation to the Services for the Customer.

2.2.2 Right to Prevent — The Service Provider has the right to prevent or limit the access of the Customer or its certain Users to the Services if the Services are being used in breach of the Documentation or the Agreement. The Service Provider exercising its right under this Clause 2.2.2 shall in no event be deemed a waiver of any other provision or prejudice any other rights of the Service Provider under the Agreement.

2.2.3 Lookalike Domains — The Service Provider purchases, registers, and maintains lookalike domain(s) to be used for the provision of the Services. For example, for the Service Provider's own internal phishing training purposes the Service Provider has registered a lookalike domain *hoaxhunt.com*. The Customer hereby consents to such registration and use by the Service Provider during the Service Term. Upon the expiration or termination of the Agreement, the Service Provider will use commercially reasonable efforts to transfer the relevant lookalike domains to a designated recipient after receiving written instructions from the Customer without delay.

2.2.4 Insurance —The Service Provider shall obtain and maintain, at its own expense, appropriate insurance coverage for the delivery of the Services, such as general liability insurance, professional liability insurance and cyber liability insurance. The Service Provider shall provide the Customer with certificates of insurance evidencing the required coverage upon request.

2.2.5 Third-Party Applications — The Services may work together with third party integrations, products, services or applications that are not owned or controlled by the Service Provider (the "Third-Party Applications"). The Customer may, at its sole discretion, choose to use such Third-Party Applications and the Customer warrants and represents that its Users with administrator rights have the authority to act on the Customer's behalf with regards to enabling and disabling any Third-Party Applications. If the Customer enables a Third-Party Application, it gives express consent to the Service Provider to transfer data, including the Customer Data (which may include Personal Data), to the third-party provider(s) of the Third-Party Application(s). Use by the Customer of Third-Party Application shall be pursuant to agreement solely between the Customer and such a third-party. The Customer is solely responsible for compliance with any terms of use of the Third-Party Application and the use of the Third-Party Applications is at the Customer's own risk. The Service Provider disclaims all liability for Third-Party Applications, including with regards to the security and privacy of the Customer Data. The Service Provider disclaims any endorsement or association with any Third-Party Applications. The Service Provider reserves the right to modify the availability of the Third-Party Application from time to time.

2.2.6 AI Features — When the Customer elects to use features of the Services which allow the Customer to utilize artificial intelligence, machine learning, or similar technologies through the Services in connection with the Customer Data (including Personal Data) (the "AI Features"), the Customer warrants and represents that its Users with administrator rights have the authority to act on the Customer's behalf with regards to enabling and disabling any AI Features. The Customer or its Users may provide input, including the Customer Data, for use with the AI Features (the "AI Input") and receive output generated and returned by the AI Features based on the AI Input (the "AI Output"). The Customer acknowledges that other customers of the Service Provider providing similar AI Input may receive the same or similar AI Output. The Customer is solely responsible for reviewing and validating the AI Output for its needs before electing to use such AI Output. The Customer shall comply with any AI Features restrictions in accordance with the Service Provider's written instructions. The Service Provider does not represent or warrant that the AI Output will be accurate, complete, error-free, or fit for a particular purpose. The Service Provider may modify the availability of the AI Features from time to time.

2.2.7 Beta Services — The Customer may choose to participate in the Beta Services or other early-stage services which are optional for the Customer to use. THE BETA SERVICES ARE NOT GENERALLY AVAILABLE AND MAY CONTAIN BUGS, ERRORS, OR DEFECTS, AND ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT WARRANTY OF ANY KIND. The Customer or the Service Provider may terminate the Customer's access to the Beta Services at any time. The Service Provider will not be liable to the Customer for damages of any kind related to the Customer's use of the Beta Services. The Beta Services are for evaluation purposes only and are not considered "Services" as defined in the Agreement.

3. Confidentiality and Non-disclosure

3.1 Mutual Confidentiality Obligations — The Parties agree to keep all Confidential Information confidential and only to use the Confidential Information for purposes of fulfilling the business affairs and transactions between the Parties contemplated by the Agreement. The Parties have the right to (i) copy Confidential Information only to the extent required in furtherance of its performance under the Agreement; (ii) deliver or disclose Confidential Information only to those Affiliates and employees who require access to the Confidential Information in order to fulfill the business affairs and transactions between the Parties contemplated by the Agreement; and (iii) deliver or disclose Confidential Information to the advisers of the Party, providing that the advisers are bound by confidentiality obligation equivalent to the confidentiality obligation defined in this Clause 3. Each Party shall only use the Confidential Information in furtherance of its performance of its rights and obligations under this Agreement, and each Party agrees not to use the other Party's Confidential Information for any other purpose.

3.2 Return of Confidential Information — Upon expiration or termination of the Agreement, or at any time upon the written request of the disclosing Party, the receiving Party shall immediately cease using the disclosing Party's Confidential Information and return, or at the election of the disclosing Party, destroy, the Confidential Information, together with all copies thereof. Notwithstanding the foregoing, both Parties have the right to keep the copies required by law or as ordered by the authorities.

3.3 Survival — The rights and obligations under this Clause 3 shall survive the termination or expiration of the Agreement, however arising, and shall remain in force for a period of five (5) years from the date of disclosure of the Confidential Information.

4. Data Protection

4.1 The Service Provider shall process the Customer's personal data pursuant to the Hoxhunt Data Processing Agreement attached as Appendix 1 (the "DPA"), which is integral part of the Agreement. In the event of any inconsistency or conflict between the terms of the other parts of the Agreement and the DPA, the DPA shall prevail.

5. Intellectual Property Rights

5.1 The Service Provider Properties — All right, title and interest, including all worldwide Intellectual Property Rights, in and to the Service Provider Properties are and shall remain the exclusive property of the Service Provider or its licensors and are protected by U.S., EU and other applicable national and international laws. For purposes of the Agreement, "Service Provider Properties" means the Services, the Documentation, and any documentation, materials, methodologies, processes, techniques, ideas, concepts, trade secrets or know-how embodied therein or that the Service Provider may develop and supply in connection with the Services or the Documentation, including all copies, portions, extracts, selections, arrangements, compilations, adaptations, modifications and improvements thereof, and all derivative works of any of the foregoing. This is not an assignment or "work for hire" agreement, and nothing in the Agreement grants to the Customer any ownership or use rights with respect to the Service Provider Properties except for the access and use rights expressly granted in the Agreement. The Customer shall not take any actions to claim or assert ownership of any Service Provider Properties or seek to register Intellectual Property Rights in or to any Service Provider Properties.

5.2 Customer Data — As between the Service Provider and the Customer, all right, title and interest in the Customer Data and all Intellectual Property Rights therein, are and shall remain the exclusive property of the Customer. The Customer hereby grants to the Service Provider the non-exclusive, royalty-free, worldwide, freely transferable (to the Service Provider's Affiliates or subprocessors) right and license to use the Customer Data and perform all acts with respect to the Customer Data: (i) as may be necessary for the Service Provider to provide and improve the Services; and (ii) as otherwise authorized by the Customer in writing. The Service Provider shall have the right to monitor and collect data from the Customer's and its Users' use of the Services for license compliance and to prevent fraud and illegal activity.

5.3 Feedback — By providing Feedback to the Service Provider, the Customer shall assign and hereby assigns all rights in and to the Feedback to the Service Provider and agrees that the Service Provider, at its sole discretion, shall have the right to freely utilize the Feedback as it deems fit as well as to develop, patent, license, distribute, sell future versions of products and services that utilize such Feedback, in whole or in part. The Service Provider is not obliged to pay any compensation to the Customer for any use of the Feedback. For the sake of clarity, the Customer has no obligation to give the Feedback, and the Service Provider has no obligation to use it or take it into account.

6. Indemnification

6.1 By Service Provider — The Service Provider shall indemnify, defend and hold harmless the Customer and its Affiliates from and against all third-party claims, demands, causes of action and liability of any kind, for damages, losses, costs and expenses, including reasonable legal fees (collectively, "Third-Party Claim") alleging that the Services infringe or misappropriate a third party's Intellectual Property Rights. Notwithstanding anything to the contrary in the Agreement, the Service Provider's obligation under this Clause 6.1 shall not apply to the extent that the Third-Party Claim arises out of (i) the Customer's breach of the Agreement; (ii) revisions to the Services made without the Service Provider's written consent; (iii) the Customer's failure to incorporate updates or upgrades at the request of the Service Provider; (iv) the Customer's use of the Services in combination with hardware or software not provided by the Service Provider, including, without limitation, the Environment of Use; or (v) infringing or illegal Customer Data. In the defense and or settlement of such a Third-Party Claim, the Service Provider may, at its option, (i) secure the right for the Customer to continue to use the Services; (ii) replace or modify the Services to make them non-infringing provided there is no material degradation to the Services; or (iii) require the Customer to stop using the Services and refund the Service Fees on a pro-rata basis for any unperformed Services. This Clause 6.1 states the Customer's and its Affiliates' and Users' sole rights and remedies and the Service Provider's (including the Service Provider's affiliates, employees, agents, and contractors) sole obligations and liability in respect of infringement of any third-party's Intellectual Property Rights.

6.2 By Customer — The Customer shall indemnify, defend and hold harmless the Service Provider and its Affiliates and licensors and their respective officers, directors and employees from and against all Third-Party Claims arising from or relating to: (i) a claim or threat that the Customer Data infringes, misappropriates or violates any third party's privacy or Intellectual Property Rights; (ii) the occurrence of any of the exclusions set forth in Clause 6.1 of these Terms; or (iii) a breach of Clause 2.1.5 of these Terms.

6.3 Indemnification Procedures — Each Party's respective indemnification obligations are conditioned upon: (i) being promptly notified in writing of any Third-Party Claim; (ii) the indemnified Party providing all reasonable assistance in the defense of such Third-Party Claim so as not to materially prejudice the defense; and (iii) the indemnifying Party is given the sole authority to defend or settle such Third-Party Claim. In no event shall an indemnified Party settle any claim without the indemnifying Party's prior written approval.

7. Payment of Service Fees

7.1 To the Service Provider — When the Services are sold directly by the Service Provider to the Customer

7.1.1 Service Fees — The Customer shall pay the Service Provider the Service Fees set out and agreed by the Parties in the applicable Order. The Customer's payment obligations are non-cancelable, and fees are non-refundable except as otherwise provided in the Agreement.

7.1.2 Invoicing — The Service Fees are invoiced annually in advance during the Service Term. Invoices shall be sent after the Agreement has been fully signed for the first Service Term, and thereafter, on the confirmation of each Service Term. Unless otherwise agreed in the Order, the term of payment is thirty (30) calendar days from receipt of an invoice. Any amounts not paid when due shall accrue interest at the lesser of one percent (1.0%) per month or the maximum rate allowed by law. If the Customer fails to pay any fee due under the Agreement, without limiting any of its other rights or remedies, the Service Provider shall have the right to suspend performance until the Service Provider receives all past due amounts from the Customer.

7.1.3 Additional Users — The Customer may add Additional Users during the Service Term, for which the Services Fees are invoiced for the remainder of the Service Term automatically. The Service Provider reserves the right to cancel any Additional Users for which the Customer has not paid the relevant Service Fees.

7.1.4 Taxes — All Service Fees are expressed exclusive of any taxes, duties or other such public fees and charges. The Customer shall be responsible for, and shall promptly pay or reimburse the Service Provider for, the payment of all sales, use, excise, withholding, value-added or similar taxes, assessments, or duties (or other similar charges) imposed by any governmental agency (including any interest and penalty imposed thereon as a result of any act or omission of the Service Provider that is in accordance with the direction or request of the Customer) that are based on or with respect to the Services or the amounts payable to the Service Provider therefor. If required by laws and regulations to be applied such amounts will be added to the Service Fees and shall be invoiced to and payable by the Customer.

7.1.5 Set-Off — All Service Fees due under the Agreement shall be paid in full without any set-off, counterclaim, deduction or withholding (other than any deduction or withholding of tax as required by law).

7.2 To the Partner — When the Services are sold through the Partner to the Customer

7.2.1 Service Fees — The Customer shall pay the Service Fees to the Partner as agreed between the Customer and the Partner.

8. Warranty Disclaimer and Limitation of Liability

8.1 Disclaimer of Warranties — EXCEPT AS SET FORTH IN THE AGREEMENT, THE SERVICE PROVIDER MAKES NO REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SERVICE PROVIDER IS NOT RESPONSIBLE FOR THE IMPACT ON THE ACCURACY, RELIABILITY, AVAILABILITY OR TIMELINESS OF RESULTS OF FACTORS OUTSIDE ITS REASONABLE CONTROL, INCLUDING THE CUSTOMER'S NETWORK ISSUES, VERSIONS OF THE CUSTOMER'S APPLICATIONS, CORRUPTED, INCOMPLETE OR INTERRUPTED DATA RECEIVED FROM THE CUSTOMER OR OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS. THE SERVICE PROVIDER IS NOT LIABLE FOR ANY DAMAGE THAT THE CUSTOMER MAY SUFFER BECAUSE OF A VIRUS, TROJAN, OR ANY MALICIOUS SOFTWARE, A SECURITY BREACH, A FAILURE OR DISRUPTION IN THE GENERAL COMMUNICATIONS NETWORK, OR SOME OTHER SIMILAR REASON, PROVIDED THAT SUCH EVENT HAS BEEN OUTSIDE THE SERVICE PROVIDER'S REASONABLE CONTROL. THE SERVICE PROVIDER IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGES RESULTING FROM SUCH PROBLEMS.

8.2 Limitation of Liability — NEITHER PARTY SHALL HAVE LIABILITY, WHETHER IN TORT (INCLUDING IN NEGLIGENCE), CONTRACT OR OTHERWISE, FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; LOSS OF PROFIT, BUSINESS, GOODWILL, REVENUE OR SAVINGS; DAMAGES PAYABLE TO THIRD PARTIES; LOSS OR ALTERATION OF DATA OR EXPENSES CAUSED THEREFROM; OR COST OF COVER PURCHASE ARISING UNDER OR IN CONNECTION WITH THE AGREEMENT, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY (INCLUDING BUT NOT LIMITED TO PRICE REFUNDS OR REDUCTIONS) TO THE OTHER PARTY ARISING OUT OF OR RELATED TO THE AGREEMENT, FOR ANY CLAIM, CAUSE OF ACTION, EVENT, ACT, OMISSION OR FAILURE OCCURRING OR ARISING DURING ANY TWELVE (12) MONTH PERIOD EXCEED THE AMOUNT OF THE NET PRICES PAID BY THE CUSTOMER TO THE SERVICE PROVIDER, OR TO THE PARTNER, FOR THE SERVICES DURING THE SAID PERIOD UNDER THE AGREEMENT. THE LIMITATIONS OF LIABILITY SHALL NOT APPLY TO: DAMAGES CAUSED BY GROSS NEGLIGENCE OR INTENTIONAL ACT, OR DEATH OR PERSONAL INJURY DUE TO NEGLIGENCE, OR BREACH OF CLAUSE 3 (CONFIDENTIALITY AND NON-DISCLOSURE) OR 6 (INDEMNIFICATION) OF THESE TERMS.

9. Service Level Agreement

9.1 Uptime Commitment — For any uptime percentage of less than 96.7% in any calendar month subject to Clause 9.2, the Customer shall be eligible for a free extra month of the Services (the "Service Credit"). The uptime percentage is calculated by subtracting from 100% the percentage of minutes during the calendar month in which the Services were unavailable to the Customer. The latest uptime statistics of the Services are available at https://status.hoxhunt.com/.

9.2 Exclusions — The Service Provider's uptime commitment is not affected by unavailability which: (i) is caused by factors outside of the Service Provider's reasonable control, including any force majeure event, Internet access, or problems beyond the demarcation point of the Service Provider's network; (ii) results from any actions or inactions of the Customer or any third party; (iii) results from the equipment, software or other technology of the Customer or any third party (other than third party equipment within the Service Provider's direct control); (iv) results from any maintenance, that the Customer has been informed about at least three (3) days prior to the maintenance break; or (v) is required by laws, regulations, authorities' orders, instructions, statements, or the recommendations of reputable industry organizations.

9.3 Claim and Sole Remedy — The Customer should submit a claim regarding the uptime percentage via email at support@hoxhunt.com. Unless otherwise provided in the Agreement, the Customer's sole and exclusive remedy for any unavailability, non-performance, or other failure by the Service Provider to provide the Services is the receipt of the Service Credit (if eligible) in accordance with this Clause 9.

10. Term and Termination

10.1 Term — The Agreement shall be in force as long as there is an active Service Term in force with the Customer. Unless otherwise agreed in the Order or between the Customer and the Partner, as relevant, after each Service Term, the Agreement shall renew automatically for additional Service Terms of one (1) year, unless either Party gives written notice of termination no less than three (3) months prior to the end of the then-current Service Term.

10.2 Termination for Cause — Both Parties have the right to terminate the Agreement with immediate effect upon written notice if (i) the other Party commits a material breach of the Agreement and does not rectify its breach, if rectifiable, within thirty (30) days of the written notification on the matter by the other Party; (ii) the other Party is insolvent, is petitioned for or applies for bankruptcy or reorganization, is a debtor in recovery proceedings, makes a transaction as an unfair preference to its claimants, or it is otherwise clear that the other Party is not able to properly fulfil its obligations due to financial difficulties or other reasons; or (iii) if the control of the Customer is transferred to a competitor of the Service Provider. Such termination shall be in addition to any other remedies that may be available to the non-breaching Party.

10.3 Other Termination — In the event it becomes illegal for the Service Provider to perform any of its obligations under the Agreement, then the Service Provider shall be excused from performance and shall have the right to suspend or terminate the Agreement upon written notice to the Customer to the extent necessary to comply with applicable laws, rules or regulations, without liability for breach or termination.

11. Governing Law and Jurisdiction

11.1 Governing Law and Jurisdiction — The Agreement shall be governed by and construed in accordance with the laws listed in the below table based on the applicable Hoxhunt contracting party, without regard to principles of conflicts of law. All disputes arising out of or in connection with the Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce. The language of arbitration shall be English, and place as listed in the below table. The United Nations Convention on Contracts for International Sale of Goods shall not apply to the Agreement. If the applicable Hoxhunt contracting party is Hoxhunt Inc., also the Uniform Commercial Code and the Uniform Computer Information Transaction Act shall not apply.

Hoxhunt contracting party:	**Governing law:**	**Place of arbitration:**
Hoxhunt Inc.	Laws of State of New York	New York, the United States
Hoxhunt GmbH	Laws of Germany	Düsseldorf, Germany
Hoxhunt Oy	Laws of Finland	Helsinki, Finland

12. Miscellaneous

12.1 Force Majeure — Except for a Party's payment obligations, neither Party is liable for delays or damage resulting from a force majeure event. A force majeure is defined as an obstacle beyond the control of either Party that the Party could not have reasonably predicted when entering into the Agreement and that the Party could not have affected or prevented via reasonable precautions. For instance, a strike, lock-out, boycott, war or a comparable armed conflict, natural catastrophes, interruption to general traffic, and legal provisions or other measures by the state that have come into effect after entering into the Agreement, and which prevent fulfilment of contractual obligations, are considered force majeure. The delay of a Party's subcontractor is also regarded as force majeure, if the delay is caused by a force majeure event. A Party shall immediately inform, in writing, the other Party of a force majeure event. The first Party shall also inform the other of the cessation of the force majeure event.

12.2 Assignment — Either Party shall have the right to transfer or assign the Agreement or any of its rights or obligations hereunder, in whole or in part, at its sole discretion to any Affiliate or in connection with the sale or transfer of its business or part thereof, and by merger or demerger, except for to the other Party's direct competitor. The Customer shall not transfer or assign the Agreement, or any rights or obligations granted hereunder, in whole or in part, without the prior written consent of the Service Provider except for as provided above.

12.3 Amendment — No change, modification, amendment or addition of or to the Agreement shall be effective unless it is in writing and approved by both Parties.

12.4 No Waiver — No failure or delay by a Party to exercise any right or remedy provided under the Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

12.5 Remedies — Except as expressly provided in the Agreement, the rights and remedies provided under the Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

12.6 Severance — If any provision or part-provision of the Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of the Agreement.

12.7 Entire Agreement — The Agreement constitutes the entire agreement between the Parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

12.8 No Partnership or Agency — Nothing in the Agreement is, unless otherwise expressly provided, intended to or shall operate to create a partnership between the Parties, or authorize either Party to act as agent for the other, and neither Party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power).

12.9 Third Party Rights — The Agreement, to the greatest extent permissible by law, does not confer any rights on any person or Party other than the Parties to the Agreement and, where applicable, their successors and permitted assigns.

12.10 Interpretation — Unless the context otherwise requires, words in the singular shall include the plural meaning and vice versa. Clause headings shall not affect the interpretation of the Agreement.

APPENDIX 1

HOXHUNT DATA PROCESSING AGREEMENT

This Hoxhunt Data Processing Agreement (the "DPA") is an integral part of the Agreement.

1. Definitions

Any capitalized terms used but not defined in this DPA will have the meaning given to such terms in other parts of the Agreement. In the DPA, the following terms have the meanings set forth below:

"Adequacy Decision"	means the adequacy decision adopted by the European Commission on the basis of the GDPR applying to the processing of the Personal Data under this DPA, including all as amended superseded or replaced from time to time;
"Data Protection Laws"	means, as applicable, the General Data Protection Regulation (the "GDPR") (Regulation (EU) 2016/679 of the European Parliament and of the Council), other applicable EU or EU member state law (and related laws in the United Kingdom and Switzerland, including the Swiss Federal Act on Data Protection of 2020 and its Ordinance (the "Swiss FADP")), California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 along with any associated regulations (the "CCPA"), or any other applicable state or national law that applies to the processing of the Personal Data under this DPA, including all as amended superseded or replaced from time to time;
"Controller" or "Business"	means the entity that determines the purposes and means of the processing of the Personal Data under this DPA, or such equivalent term as defined by the Data Protection Laws (collectively defined herein as the "Controller");
"Data Subject"	means the identified or identifiable natural person who is the subject of the Personal Data, or such equivalent term as defined by the Data Protection Laws;
"Personal Data"	means any information constituting "personal information", "personal data" or "personally identifiable information" of the Data Subject which is provided to and processed by the Processor on behalf of the Controller under this DPA, or such equivalent term as defined by the Data Protection Laws;
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data processed under this DPA, or such equivalent term as defined by the Data Protection Laws;
"Processor" or "Service Provider"	means the entity that processes the Personal Data on behalf of the Controller under this DPA, or such equivalent term as defined by the Data Protection Laws (collectively defined herein as the "Processor");
"Standard Contractual Clauses"	means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR adopted by the European Commission applying to the processing of the Personal Data under this DPA, including all as amended or replaced from time to time;
"Subprocessor"	means other processor engaged by the Processor and/or its Affiliate to process the Personal Data under this DPA, or such equivalent term as defined by the Data Protection Laws;
"Supervisory Authority"	means any competent supervisory authority under the Data Protection Laws; and
"UK Addendum"	means the international data transfer addendum to the Standard Contractual Clauses issued by the UK Information Commissioner's Office (the "ICO") pursuant to the Data Protection Act 2018, applying to the processing of the Personal Data under this DPA, including all as amended or replaced from time to time.

2. Scope

2.1 With regard to the processing of the Personal Data under this DPA, the Customer is the Controller, and the Service Provider is the Processor. The Processor shall process the Personal Data on behalf of the Controller only for the purpose of and to the extent required for providing the Services specified in the Agreement. The details of the processing of the Personal Data are specified in Annex 1 of this DPA.

3. Controller Obligations

3.1 The Controller shall:

(i) process the Personal Data in compliance with the Data Protection Laws and good data processing practices, and comply at all times with the obligations applicable to the Controller;

(ii) ensure that this DPA is not unlawful and does not violate the rights of third parties, and that the Controller's instructions for the processing of the Personal Data comply with the Data Protection Laws;

(iii) retain the right to take reasonable and appropriate steps to (i) ensure that the Processor processes the Personal Data in a manner consistent with the Data Protection Laws, and (ii) upon notice, stop and remediate any unauthorized processing of the Personal Data, including any use of the Personal Data not expressly authorized in this DPA; and

(iv) have sole responsibility for the means by which the Controller shall acquire the Personal Data.

4. Processor Obligations

4.1 The Processor shall:

(i) process the Personal Data with all due care and skill, and in a workmanlike manner in accordance with good data processing practices and in compliance with this DPA and the Data Protection Laws;

(ii) process the Personal Data in accordance with the Controller's documented instructions as necessary for the performance of the Services and this DPA, unless required to do otherwise by any applicable law, court of competent jurisdiction or the Supervisory Authority, in which case, the Processor shall inform the Controller of such requirement before processing of the Personal Data, unless such notification is prohibited;

(iii) inform the Controller if, in its opinion, the Controller's documented instructions infringe the Data Protection Laws or any other applicable law or if the Processor determines that it can no longer meet its obligations under the Data Protection Laws;

(iv) ensure that persons authorized by the Processor to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(v) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing the Personal Data as described in Annex 2 of this DPA;

(vi) assist the Controller by appropriate technical and organizational measures, to a commercially reasonable extent and provided that the Controller does not otherwise have access to such information, for the fulfillment of the Controller's obligation to respond to requests for exercising the Data Subject's rights;

(vii) delete or return, at the choice of the Controller, and upon the Controller's written request, all the Personal Data to the Controller after the end of the provision of the Services (provided, however, that certain automated backups may be stored longer) relating to the processing, and delete existing copies unless any applicable law requires storage of the Personal Data;

(viii) assist the Controller, to a commercially reasonable extent and provided that the Controller does not otherwise have access to such information, in ensuring compliance with the Controller's obligations under the Data Protection Laws, such as with the Controller's obligation to perform a data protection assessment or to consult with the Supervisory Authority as set out by the Data Protection Laws;

(ix) make available to the Controller all information necessary to demonstrate compliance with the Processor's obligations under this DPA, and allow for and contribute to the necessary audits, including remote inspections, conducted by the Controller or another auditor mandated by the Controller at the Controller's cost provided that the Processor shall accept the scope, methodology, timing and conditions of such audits in advance;

(x) not "sell" or "share" or use the Personal Data for purposes of "targeted advertising" (as such terms are defined in the Data Protection Laws), or combine the Personal Data with other personal data that the Processor may obtain outside of the Services except as permitted by the Data Protection Laws; and

(xi) not retain, use, or disclose the Personal Data outside of the direct business relationship between the Controller and the Processor unless otherwise agreed in the Agreement.

4.2 In case the Data Subject or the Supervisory Authority make a request concerning the Personal Data, including a request for restricting, erasing or correcting the Personal Data, delivering them any information or executing any other actions, the Processor shall, without undue delay, inform the Controller on all such requests prior to any response or other action concerning the Personal Data, or afterwards as soon as reasonably possible in case the Data Protection Laws prescribe an immediate response. The Processor may only restrict, erasure or correct such Personal Data when instructed to do so by the Controller or required by the Data Protection Laws.

4.3 In the event of the Personal Data Breach, the Processor shall without undue delay but no later than in forty-eight (48) hours after becoming aware of such Personal Data Breach, notify the Controller about the Personal Data Breach to its designated contact details provided below. To the extent available, this notification shall include the Processor's then-current assessment of the following: (i) the nature of the Personal Data Breach, including, where possible, the categories and approximate number of the Data Subjects concerned and the categories and approximate number of the Personal Data records concerned; (ii) the likely consequences of the Personal Data Breach; and (iii) measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects. The Processor shall provide timely and periodic updates to the Controller as additional information regarding the Personal Data Breach becomes available. The Controller acknowledges that any updates may be based on incomplete information. The Processor shall use all reasonable endeavors to protect the Personal Data after having become aware of the Personal Data Breach and investigate the Personal Data Breach to identify the cause, minimize harm, and prevent a recurrence.

Contact for the Controller:
The same as included in the Order unless provided separately in writing to the Processor.

Contact for the Processor:
Hoxhunt Legal
legal@hoxhunt.com

5. International Transfers

5.1 If a country outside the borders of the European Economic Area (the "EEA"), Switzerland, or the United Kingdom offers an adequate level of data protection based on the Adequacy Decision, the Personal Data may be transferred by the Processor to such country without any further safeguard being necessary.

5.2 If a country outside the borders of the EEA, Switzerland, or the United Kingdom does not offer an adequate level of data protection based on the Adequacy Decision, the Processor shall be entitled to transfer the Personal Data outside the borders of the EEA, Switzerland, or the United Kingdom only with the Controller's written consent and provided that such transfer is undertaken on the applicable basis provided for in the Data Protection Laws. In the case the Standard Contractual Clauses or other relevant transfer instrument are required between the Controller and the Processor for such a transfer, the applicable transfer instrument shall be incorporated and deemed entered in respect of the Personal Data transfer based on the information provided in this DPA. Under this DPA, the Controller gives its written consent to the Processor to transfer the Personal Data outside the borders of the EEA, Switzerland, or the United Kingdom to the Subprocessors specified in Annex 1 of this DPA.

6. Subprocessors

6.1 By entering into this DPA, the Controller gives its written consent to the Processor to engage the Subprocessors specified in Annex 1 of this DPA to perform processing activities on the Personal Data.

6.2 The Processor may update its list of the engaged Subprocessors from time to time and the Processor shall notify the Controller of such update with reasonable notice. The Controller may object to the appointment of a new Subprocessor on reasonable grounds in writing within fourteen (14) days from the date of the notification. In such a case the Processor may offer an alternative Subprocessor to the Controller. If the Processor chooses not to offer an acceptable alternative Subprocessor, the Controller may terminate the elements of the Services that cannot be delivered without the objected Subprocessor.

6.3 The Processor shall ensure that all Subprocessors are bound by contractual obligations at least as robust as those in this DPA with respect to the protection of the Personal Data, and the Processor shall remain fully liable to the Controller for the performance of the Subprocessor data protection obligations under this DPA.

7. Indemnification

7.1 The Processor shall indemnify, defend and hold harmless the Controller against any third-party claims or administrative sanctions brought pursuant to the Data Protection Laws against the Controller resulting from the Processor's breach of this DPA up to the aggregate value of USD 1,000,000 (converted into the Controller's local currency), provided that (i) the Processor is given prompt notice of any such claim or possible sanction; (ii) the Controller provides reasonable cooperation in relation the defense and settlement of such claim or possible sanction so as not to materially prejudice the defense; and (iii) the Processor is given the sole authority to defend or settle such claim and/or make representations to the relevant authorities in relation to any possible sanction. This Clause 7 of this DPA states the Controller's sole and exclusive rights and remedies and the Processor's entire obligations and liability from a breach of this DPA.

8. Governing Law and Jurisdiction

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

ANNEX 1 OF THE DPA

The details of the processing of the Personal Data are specified in this Annex 1.

The categories of Data Subjects whose Personal Data is processed: The categories of Data Subjects whose Personal Data is processed are the Users of the Services authorized and appointed by the Controller.

The categories of the Personal Data processed: The categories of the Personal Data processed include the following mandatory and optional categories of Personal Data provided at the discretion of the Controller:

Mandatory:	**Optional:**
- Full name; - Email address; - Geolocation based on IP; - Last data processing activity (time stamp); - Preferred languages; - Browser language; and - Employee performance statistics in the Services (such as reporting a simulated attack or completing a training package).	- Telephone numbers; - Time zone; - Employee-related information (such as a country, site, department, title, and manager); - Employee-generated content and preferences; and - Employee-related information from other systems of the Controller regarding signals of security behaviors.

The nature and purpose of the Personal Data processing: The nature and purpose of the Personal Data processing is the execution of the Services by the Processor as defined in the Agreement.

The frequency and duration of the Personal Data processing: The frequency and duration of the Personal Data processing is continuously, and as long as the Services are provided under the Agreement to the Controller.

The approved Subprocessors of the Processor: In the table below, the "Service Data" include (i) the user-reported threat data which consist of non-simulated suspected malicious emails reported by the Users that may contain Personal Data, and (ii) the "User Data" which consist of the Personal Data categories stated above.

Entity:	**Service:**	**Purpose:**	**Personal Data category processed:**	**Personal Data processing location:**	**International transfer instrument (if applicable):**
Google Cloud EMEA Ltd.	Cloud service and AI-provider	To provide the infrastructure to host the Services	Service Data	EEA	N/A
Amazon Web Services EMEA SARL	Cloud service provider	To transmit simulation content (such as simulated emails) to the Users	User Data	EEA	N/A
Cloudflare Inc.	Content Delivery Network ("CDN"), Domain Name System ("DNS"), and security services provider	To provide CDN, security and DNS services for web traffic transmitted to and from the Services	IP address	EEA and US	Where applicable, the Adequacy Decision or the Standard Contractual Clauses
MongoDB Ltd.	Database service provider	To provide the database platform hosted on Google's infrastructure	Service Data	EEA	N/A
Functional Software Inc. d/b/a Sentry	Error tracking service provider	To provide real-time error tracking and the insight needed to reproduce and fix the Services	IP address, user-agent, and user ID	US	Where applicable, the Adequacy Decision or the Standard Contractual Clauses
Zendesk Inc.	Customer support service provider	To provide way for the Users to contact the Hoxhunt support, and to triage the potential issue	User Data	EEA	N/A

Merge API Inc.	Unified API integration provider	To provide integrations to third party service providers	User Data	EEA	N/A
Hoxhunt Oy (applicable unless acting as the Processor)	All Hoxhunt services	Overall responsibility for the provision of the Services	Service Data	EEA	N/A

ANNEX 2 OF THE DPA

The details of the technical and organizational measures implemented by the Processor are specified in this Annex 2.

Physical Access Control: The Processor shall take proportionate measures to prevent unauthorized physical access to the Processor's premises and facilities holding the Personal Data.	Measures shall include: - Procedural and/or physical access control systems - Door locking or other electronic access control measures - Alarm system, video/CCTV monitor, or other surveillance facilities - Logging of facility entries/exits - ID, key, or other access requirements
Access Control to Systems: The Processor shall take proportionate measures to prevent unauthorized access to systems holding the Personal Data.	Measures shall include: - Password procedures, e.g., requirements for length or special characters, and forced password changes on a frequent basis - Access to systems subject to approval from IT system administrators - No access to systems for guest users or anonymous accounts - Central management of system access through IAM - Restrictions on the use of removable media, e.g., memory sticks, CD/DVD disks, or portable hard drives, and requirements of encryption
Access Control to Data: The Processor shall take proportionate measures to prevent unauthorized users from accessing data beyond their authorized access rights, and to prevent unauthorized access to or removal, modification, or disclosure of Personal Data.	Measures shall include: - Differentiated access rights, defined according to duties - Automated logging of user access via IT systems
Disclosure Control: The Processor shall take proportionate measures to prevent unauthorized access, alteration or removal of Personal Data during transfer of Personal Data.	Measures shall include: - Use of state-of-the-art encryption for all electronic transfers of Personal Data - Encryption using a VPN or HTTPS for remote access, transport, and communication of Personal Data
Availability Control: The Processor shall take proportionate measures to ensure that the Personal Data is protected from accidental destruction or loss.	Measures shall include: - Frequent backup of Personal Data - Remote storage - Use of anti-virus/firewall protection - Monitoring systems and devices to detect malware using EDR software - Business continuity procedures
Responsible Development and Usage of AI: The Processor shall adhere to policies and procedures for developing and using artificial intelligence technology in a manner that promotes transparency, accountability, and human interpretability.	Measures shall include: - Regular monitoring of the performance of its services that involve artificial intelligence technology
Training and Awareness: The Processor shall ensure that its employees are aware of routines on security and confidentiality.	Measures shall include: - Relevant clauses in employment contracts on confidentiality, security, and compliance with internal routines - Internal routines and courses on requirements of processing of Personal Data to create awareness

ANNEX 3 OF THE DPA

The details of the international Personal Data transfer instruments are specified in this Annex 3.

The data exporter in relation to the Personal Data transfer: The data exporter is the Customer, as specified in the Agreement, acting in the role of the Controller.

The data importer in relation to the Personal Data transfer: The data importer is the Service Provider as specified in the Agreement, acting in the role of the Processor.

The Alternative Transfer Instrument: In the event that the Processor adopts an alternative data transfer instrument (including any new version of, or successor to, the Standard Contractual Clauses) not described in this DPA (the "Alternative Transfer Instrument"), the Alternative Transfer Instrument shall apply instead of the transfer instruments described in this DPA.

EEA transfer instrument: To the extent legally required, the Controller and the Processor are deemed to have signed the Standard Contractual Clauses which form part of this DPA and are completed based on the information provided in the DPA.	Completed as specified below: - Module 2 (transfer from the Controller to the Processor) shall apply - Clause 7, the optional docking clause shall not apply - Clause 9, option 2 shall apply, and the period for prior notice of Subprocessor changes is set forth in Clause 6 of this DPA - Clause 11, the optional redress language shall not apply - Clause 13, select the Office of the Data Protection Ombudsman in Finland as a supervisory authority - Clause 17, option 1 shall apply and select the law of Finland - Clause 18, select the courts of Finland - Annexes 1, 2 and 3 of this DPA contain the information required in Annexes I, II and III
UK transfer instrument: To the extent legally required, the Controller and the Processor are deemed to have signed the UK Addendum which form part of this DPA and are completed based on the information provided in the DPA.	Completed as specified below: - The Standard Contractual Clauses completed above shall be amended as specified by the UK Addendum - Annexes 1, 2 and 3 of this DPA contain the information required in Tables 1, 2 and 3 in Part 1 - Table 4 in Part 1 shall be deemed completed by selecting "Importer"
Swiss transfer instrument: To the extent legally required, the Controller and the Processor are deemed to have signed the Standard Contractual Clauses in accordance with the Swiss FADP which form part of this DPA and are completed based on the information provided in the DPA.	Completed as specified below: - The Standard Contractual Clauses completed above shall be amended as specified by the Swiss FADP - References to the GDPR in the Standard Contractual Clauses are to be understood as references to the Swiss FADP insofar as the data transfers are subject exclusively to the Swiss FADP and not to the GDPR - The term "member state" in Standard Contractual Clauses shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses - The supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the Swiss FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the Standard Contractual Clauses (where the Swiss FADP and the GDPR apply, respectively)