Hoxhunt Data Processing Agreement

UNLESS OTHERWISE AGREED IN THE AGREEMENT, THIS HOXHUNT DATA PROCESSING AGREEMENT IS AN INTEGRAL PART OF THE AGREEMENT AND SHALL 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 this 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on the basis of the GDPR applying to the processing of the Personal Data under this DPA, including all as amended superseded or replaced from time to time;
“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 the applicable agreement pursuant to which the Services are provided to the Customer, and which refers to this DPA;
“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state or national law that applies to the processing of the Personal Data under this DPA, including all as amended superseded or replaced from time to time;
“DPA”	means this Hoxhunt Data Processing Agreement;
“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”);
“Customer”	means a legal entity end-customer using the Services;
“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;
“Hoxhunt”	means the Service Provider;
“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;
“Party”	means the Service Provider or the Customer, collectively referred to as the “Parties”;
“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”	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”);
“Services”	means the information, documents and services the Service Provider provides to the Customer under the Agreement;
Service Provider”	means the applicable Hoxhunt legal entity as identified in the Order. If no such entity is specified in the Order, the Service Provider shall be determined based on the Customer’s address as follows: Hoxhunt Inc. (EIN: 61-2044575), if the Customer’s address is in the United States or Canada; or Hoxhunt GmbH (HRB 105923, Amtsgericht Düsseldorf), if the Customer’s address is in Germany; or Hoxhunt Oy (Business ID: 2758722-7), if the Customer’s address is in any other country;
“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;
"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; 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. 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 or otherwise provided 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 Clause 6 of this DPA.

6. Subprocessors

6.1 The Processor may engage the Subprocessors to perform processing activities on the Personal Data. By entering into this DPA, the Controller provides its written consent for the Processor to engage the Subprocessors specified at https://hoxhunt.com/legal/subprocessors (version 1.0).

6.2 The Processor may update its 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 solely from the Processor’s breach of this DPA, up to the greater of:

(a) five (5) times the net prices paid by the Controller to the Processor, or to the Partner, for the Services during the twelve (12) month period preceding the claim under the Agreement; or

(b) ten thousand (10,000) euros (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

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 - User performance statistics in the Services (such as reporting a simulated attack or completing a training package).	- Telephone numbers; - Time zone; - Work-related information (such as a country, site, department, title, and manager); - User-related media (such as audio, and video content); - User-generated content and preferences; and - User-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.

Annex 2

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

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 - This DPA contains 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 - This DPA contains 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)