Hoxhunt Data Processing Agreement ("DPA")

1. Definitions

The same definitions in other parts of the Agreement shall also apply to this DPA. Any terms not defined herein shall be given the meaning allocated to them in the Data Protection Laws from time to time. In addition, the following terms have the meanings set forth below:

1.1 "Agreement" means the applicable agreement between the Service Provider and the Customer, to which this DPA is an integral part of;

1.2 "Data Controller" means the Customer;

1.3 "Data Processor" means the Service Provider;

1.4 "Data Protection Laws" means the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council), other applicable EU or EU member state law, or any other applicable law that applies to the processing of the Personal Data under this DPA, including all as amended superseded or replaced from time to time;

1.5 "Data Subject" shall have the same meaning as defined by the Data Protection Laws;

1.6 "Personal Data" shall have the same meaning as defined by the Data Protection Laws;

1.7 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

1.8 "Standard Contractual Clauses" means the contractual clauses issued by the European Commission by the decision (EU) 2021/914 for international transfers of Personal Data including as amended or replaced from time to time; and

1.9 "Supervisory Authority" means any competent authority under the Data Protection Laws.

2. Scope and Duration of Processing

2.1 The Data Processor shall process the Personal Data on behalf of the Data Controller only for the purpose of and to the extent required for providing the Services under the Agreement. The Personal Data shall be processed as long as the Services are provided under the Agreement. The categories of Personal Data processed under this DPA are specified in Annex 1 of this DPA.

3. Data Controller Obligations

3.1 The Data Controller shall:

i. process the Personal Data in compliance with the Data Protection Laws and good data processing practices; and

ii. ensure that all data processing by the Data Processor in accordance with this DPA and the Agreement is not unlawful and does not violate the rights of third parties.

4. Data Processor Obligations

4.1 The Data Processor shall:

i. process the Personal Data with all due care and skill, diligence and prudence, in a workmanlike manner in accordance with good data processing practices and high professional standards and in compliance with the Agreement, this DPA and the Data Protection Laws;

ii. process the Personal Data only on documented instructions from the Data Controller, including with regard to transfers of the Personal Data to a third country or an international organization, unless required to do so by the law to which the Data Processor is subject. In such case, the Data Processor shall inform the Data Controller of such requirement under the Data Protection Laws before processing of the Personal Data, unless that law prohibits such notification on important grounds of public interest;

iii. ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

iv. take steps to ensure that any natural person acting under the authority of the Data Processor who has access to the Personal Data does not process them except on instructions from the Data Controller, unless they are required to do so by the law;

v. implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing the Personal Data;

vi. assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights;

vii. deletes or returns, at the choice of the Data Controller, all the Personal Data to the Data Controller after the end of the provision of the Services relating to the processing, and deletes existing copies unless the law requires storage of the Personal Data;

viii. assist the Data Controller in ensuring compliance with its legal obligations, such as, with the Data Controller's data security, data protection assessment and prior consulting obligations set out by the Data Protection Laws;

ix. provide the Data Controller with necessary information in its possession for the completion of data protection impact assessments, to a reasonable extent and frequency and provided that the Data Controller does not otherwise have access to the information;

x. make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this Clause 4.1 and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller at the Data Controller's cost. The Data Processor shall inform the Data Controller if, in its opinion, an instruction infringes the Data Protection Laws or other applicable data protection provisions; and

xi. have the right to amend this DPA from time to time, and shall notify the Data Controller of such amendments as required by the Data Protection Laws.

4.2 In case the Data Subject or 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 Data Processor shall, without undue delay, inform the Data 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 prescribes an immediate response. The Data Processor may only restrict, erasure or correct the Personal Data processed on behalf of the Data Controller when instructed to do so by the Data Controller or required by the Data Protection Laws.

4.3 In the event of a Personal Data Breach, the Data Processor shall without undue delay but no later than in forty-eight (48) hours after becoming aware of it, notify the Data Controller in writing to its designated contact details provided below. The Data Processor shall use all reasonable endeavors to protect the Personal Data after having become aware of the Personal Data Breach.

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

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

5. International Transfers

5.1 Unless a country outside the borders of the European Economic Area ("EEA") offers an adequate level of data protection based on a decision by the European Commission, the Data Processor is entitled to transfer the Personal Data outside the borders of the EEA only with the Data Controller's express written consent, and provided that the Data Processor ensures that the transfer is protected by appropriate safeguards and supplementary measures as mandated from time to time by the Data Protection Laws. Where the Data Protection Laws require appropriate safeguards, the applicable Standard Contractual Clauses are incorporated and deemed entered into in respect of the transfer. By entering into this DPA, the Data Controller gives consent to the Data Processor to transfer the Personal Data outside the borders of the EEA to the sub-processors listed at Annex 1 of this DPA. Where the Data Protection Laws require supplementary measures, the Data Processor shall pseudonymize the Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject.

6. Sub-processors

6.1 By entering into this DPA, the Data Controller agrees that the Data Processor may engage the sub-processors listed at Annex 1 of this DPA. The Data Controller acknowledges that the Data Processor may update this list of sub-processors from time to time, and that the Data Processor shall notify the Data Controller of any such update with reasonable notice. The Data Controller may object to the appointment of a new sub-processor on reasonable grounds in writing within fourteen (14) or fewer calendar days from the date of notification. In such case the Data Processor shall use reasonable endeavors to secure, within a

reasonable timeframe, an alternative sub-processor so as to avoid any degradation or interruption of the Services without imposing any substantial commercial burden on either Party. If the Data Processor is unable to secure an alternative sub-processor, the Data Controller may terminate the elements of the Services that cannot be delivered without the objected sub-processor. The Data Processor shall ensure that all sub-processors are bound by contractual obligations at least equivalent to this DPA with respect to the protection of the Personal Data, and the Data Processor shall remain fully liable to the Data Controller for the performance of the sub-processor data protection obligations under this DPA.

7. Applicable Law and Jurisdiction

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

Annex 1 of the DPA

Categories of the Data Subjects whose Personal Data is processed — The categories of Data Subjects, which are affected by the Personal Data processing within the framework of this Agreement are the users of the Services authorized and appointed by the Data Controller.

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

Mandatory:
- Full name;
- Email address;
- Geolocation based on IP;
- Last data processing activity (time stamp);
- Native language;
- Browser language; and
- Employee performance statistics in the Services (such as reporting a simulated attack or completing a training package).

Optional:
- Telephone numbers;
- Spoken languages;
- 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 Data Controller regarding signals of security behaviors.

Subject-matter, nature, and purpose of the Personal Data processing — The execution of the Services by the Data Processor as defined in the Agreement.

Frequency and duration of the Personal Data processing — Continuously, and as long as the Services are provided under the Agreement to the Data Controller.

Approved sub-processors of the Data Processor — In the below table, 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 Safeguard (if applicable)	Security Certification
Infrastructure as a Service ("IaaS") and Platform as a Service ("PaaS")						
Google Cloud EMEA Ltd.	Cloud service provider	To provide the infrastructure to host the Services	Service Data	EEA	N/A	ISO/IEC 27001, ISO/IEC 27701, SOC 2
Amazon Web Services EMEA SARL	Cloud service provider	To transmit simulation content (such as simulated emails) to the users	User Data	EEA	N/A	ISO/IEC 27001, ISO/IEC 27701, SOC 2
Cloudflare Inc.	Content Delivery Network ("CDN"), Domain Name System ("DNS"), and security services	To provide CDN, security and DNS services for web traffic transmitted to and from the Services	IP address	EEA, and US	EU SCC	ISO/IEC 27001, ISO/IEC 27701, SOC 2

MongoDB Ltd.	Database service	To provide the database platform hosted on Google's infrastructure	Service Data	EEA	N/A	ISO/IEC 27001, SOC 2
Service Supporting						
Functional Software Inc. d/b/a Sentry	Error tracking service	To provide real-time error tracking and the insight needed to reproduce and fix the Services	IP address, user-agent, and user ID	US	EU SCC, and the transferring is not systematic as Sentry is only involved in error cases	ISO/IEC 27001, SOC 2
Zendesk Inc.	Customer support service	To provide way for the users to contact the Hoxhunt customer support, and to triage the potential issue	User Data	EEA	N/A	ISO/IEC 27001, ISO/IEC 27701, SOC 2
Hoxhunt Oy (unless acting as the Data Processor)	All Hoxhunt services	Overall responsibility for the provision of the Services	Service Data	EEA	N/A	SOC 2