DOT (SNOWBOARD SOFTWARE GMBH)
PRIVACY AND SECURITY

We are committed to protecting you and your data

Snowboard Software GmbH is committed to meeting the requirements of the General Data Protection Regulation ('GDPR'). The GDPR is a landmark EU data privacy law, effective May 2018, which affects both European and non-European businesses. The GDPR expands user data privacy rights and standards for any organization that handles EU citizens' personal data, regardless of its location.

Description of product and services

Snowboard Software GmbH’s product Dot is a chat agent that helps members of organization answer their data questions in natural language.

Snowboard Software's data processing addendum ('DPA')

Dot's DPA is available to all organizations using its software. The DPA certifies that Snowboard will process all personal data in accordance with the applicable data protection laws, including GDPR requirements. The DPA can be found below.

Snowboard Software's security infrastructure

It is our utmost priority to keep our customers' sensitive data and information safe. Snowboard Software GmbH is committed to meeting the requirements of SOC 2 Type I and SOC 2 Type II. Snowboard Software adheres to industry-leading standards to manage our network, secure our application, and set policies across our organization. Details about security policies can be found below.

Stay in the loop

This page will be revised over time to reflect any privacy and security related updates. If you have questions, please reach out to us at hi@sled.so.

DATA PROCESSING ADDENDUM (DPA)

This Data Processing Agreement (“Agreement“) forms part of the Contract for Services (“Principal Agreement“) between ____ (the “Company”) and Snowboard Software GmbH (referred equally as ‘Dot’, ‘Sled’ or ‘Snowboard’) (the “Data Processor”) (together as the “Parties”) and is incorporated into Snowboard Software GmbH's Terms of Service.

WHEREAS
(A) The Company acts as a Data Controller.
(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.
(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
(D) The Parties wish to lay down their rights and obligations.

Snowboard Software GmbH:	**:**
By:	**By:**
Name: Theo Tortorici	**Name:**
Title: Co-Founder and Managing Director	**Title:**
Date:	**Date:**

IT IS AGREED AS FOLLOWS

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 “Agreement” means this Data Processing Agreement and all Schedules;

1.1.2 “Company Personal Data” means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 “Contracted Processor” means a Sub-processor;

1.1.4 “Data Protection Laws” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 “EEA” means the European Economic Area;

1.1.6 “EU Data Protection Laws” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 “GDPR” means EU General Data Protection Regulation 2016/679;

1.1.8 “Data Transfer” means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 “Services” means those services and activities to be supplied to or carried out by or on behalf of Snowboard Software GmbH for Customer pursuant to the Agreement.

1.1.10 “Sub-processor” means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall: 2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and 2.1.2 not Process Company Personal Data other than on the relevant Company’s documented instructions. `

2.2 The Company instructs Processor to process Company Personal Data.

3. Processor

3.1 Personnel Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub-processing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Sub-processor unless required or authorized by the Company.

5.2 Processor engages the organizations or persons listed above to process Customer Data (each a "Sub-processor," and the list at the foregoing URL, the "Sub-processor List") to help Dot satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Sub-processors. Customer hereby consents to the use of such Sub-processors. In the event that Dot seeks to use additional Sub-processors and update the Sub-processor List, Dot will provide notice of such additional Sub-processors to you (which mayb be via email, a posting or notification on an online portal for our services or other reasonable means). In the event that you do not wish to consent to the use of such additional Sub-processor, you may notify Dot that you do not consent within fifteen (15) days on reasonable grounds relating to the protection of Customer Data by following the instructions set forth in the Sub-processor List or contacting privacy@Dot.com. In such case, Dot shall have the right to cure the objection through one of the following options:

5.2.1 Dot will cancel its plans to use the Sub-processor with regards to processing Customer Data or will offer an alternative to provide its Services or services without such Sub-processor;

5.2.2 Dot will take the corrective steps requested by you in your objection notice and proceed to use the Sub-processor;

5.2.3 Dot may cease to provide, or you may agree not to use whether temporarily or permanently, the particular aspect or feature of the Dot Services or services that would involve the use of such Sub-processor; or

5.2.4 you may cease providing Customer Data to Dot for processing. If none of the above options are commercially feasible, in Dot's reasonable judgment, and the objection(s) have not been resolved to the satisfaction of the parties within thirty (30) days of Dot's receipt of your objection notice, then either party may terminate any subscriptions, order forms or usage regarding the Services or Dot services for cause and in such case, you will be refunded any pre-paid fees for the applicable subscriptions, order forms or usage to the extent they cover periods or terms following the date of such termination. Such termination right is your sole and exclusive remedy if you object to any new Sub-processor.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.3 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection

8.1 Impact Assessment and Prior Consultation Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:(a) disclosure is required by law;(b) the relevant information is already in the public domain.

12.2 Notices._All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of the EU member state where the data exporter is established.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of the EU member state in which the data exporter is established.

14. Standard Contractual Clauses.

14.1 Dot will process Customer Data that originates in the European Economic Area in accordance with the standard contractual clauses adopted by the EU Commission on June 4, 2021 ("EU SCCs") which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

14.1.1 Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller

14.1.2 and Dot is processing Customer Data as a processor.

14.1.3 Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Dot is processing Customer Data as a sub-processor.

14.2 For each module of the EU SCCs, where applicable, the following applies:

14.3 The optional docking clause in Clause 7 does not apply;

14.4 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 1(g) of this DPA.

14.5 In Clause 11, the optional language does not apply;

14.6 All square brackets in Clause 13 are hereby removed;

14.7 In Clause 17 (Option 1), the EU SCCs will be governed by the EU member state where the data exporter is located;

14.8 In Clause 18(b), disputes will be resolved before the courts of the EU member state where the data exporter is located;

14.9 Exhibit A to this DPA contains the information required in Annex I and Annex III of the EU SCCs;

14.10 Exhibit B to this DPA contains the information required in Annex II of the EU SCCs; and

14.11 Customer Data originating from Switzerland shall be processed in accordance with the EU SCCs with the following amendments:

14.12 "FDPIC" means the Swiss Federal Data Protection and Information Commissioner.

14.13 "Revised FADP" means the revised version of the FADP of 25 September 2020, which is

14.14 scheduled to come into force on 1 January 2023.

14.15 The term "EU Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

14.16 The EU SCCs also protect the data of legal entities until the entry into force of the Revised FADP.

14.17 The FDPIC shall act as the "competent supervisory authority" insofar as the relevant data

14.18 transfer is governed by the FADP

14.19 With respect to Customer Data originating from the United Kingdom, the parties will comply with the terms of Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2

February 2022, as it is revised under Section 18 of those Mandatory Clauses (the “UK Addendum”). The parties also agree (i) that the information included in Part 1 of the UK Addendum is as set out in Annex I of Appendix A to this DPA and (ii) that either party may end the UK Addendum as set out in Section 19 of the UK Addendum.

Exhibit A
ANNEX I

A. LIST OF PARTIES

Data exporter(s): the Services customer identified in this DPA
Data importer(s): the Services provider identified in this DPA

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Users of data exporters applications.

Categories of personal data transferred
Name, contact information, demographic information, or other information provided by the user in unstructured or structured data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
No sensitive data is intended to be transferred unless the user includes it unexpectedly in unstructured and structured data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Continuous.

Nature of the processing
The performance of the services described in the agreement to which this appendix is attached.

Purpose(s) of the data transfer and further processing
The performance of the services described in the agreement to which this appendix is attached.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
During the term of the agreement
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing. The performance of the services described in the agreement to which this appendix is attached.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13
The data protection authority of the EU Member State in which the exporter is established.

Exhibit B
ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

To learn more about Dot's technical and organizational security measures to protect Customer Data, . The Security Measures below include the subset of the information available upon request which applies to this DPA.

SECURITY MEASURES

1. **Corporate Identity, Authentication, and Authorization Controls.**

1.1 Dot maintains industry best practices for authenticating and authorizing internal employee and service access, including the following measures:

- Mandatory multi-factor authentication is used for authenticating to Dot's identity provider.
- Unique login identifiers are assigned to each user;
- Established review and approval processes for any access requests to services storing Customer Data;
- Periodic access audits designed to ensure access levels are appropriate for the roles each user performs;
- Established procedures for promptly revoking access rights upon employee separation;
- Established procedures for reporting and revoking compromised credentials such as passwords and API keys); and
- Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.

1.2 Dot maintains industry best practices for authenticating and authorizing customers to the Services, including the following measures:

- Use of a third-party identity access management service to manage Customer identity, meaning Dot does not store user-provided passwords on users' behalf; and
- Logically separating Customer Data by organization account using unique identifiers. Within an organization account, unique user accounts are supported
- Cloud Infrastructure and Network Security. Dot maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:
- Separate production and non-production environments;
- Primary backend resources are deployed behind a VPN.
- The Services are routinely audited for security vulnerabilities.
- Application secrets and service accounts are managed by a secrets management service;
- Network security policies and firewalls are configured for least-privilege access against a pre- established set of permissible traffic flows. Non-permitted traffic flows are blocked; and
- Services logs are monitored for security and availability.

2. **System and Workstation Control.**

Dot maintains industry best practices for securing Dot's corporate systems, including laptops and on-premises infrastructure, including:

- Endpoint management of corporate workstations;
- Endpoint management of mobile devices;
- Automatic application of security configurations to workstations;
- Mandatory patch management; and
- Maintaining appropriate security logs.

3. **Data Access Control.**

Dot maintains industry best practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment; and
- Customer Data submitted to the Services is only used in accordance with the Dot Privacy Policy and Terms of Use and the terms of the DPA, Agreement, and any other contractual agreements in place with Customer.

4. **Disclosure Control.**

Dot maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:

- Encryption of data at rest in production datastores using strong encryption algorithms;

- Encryption of data in transit;
- Audit trail for all data access requests for production datastores;
- Full-disk encryption required on all corporate workstations;
- Device management controls required on all corporate workstations;
- Restrictions on use of portable or removable media; and
- Customer Data can be deleted upon request at hi@sled.so

5. **Availability control.**

Dot maintains industry best practices for maintaining Services functionality through accidental or malicious intent, including:

- Ensuring that systems may be restored in the event of an interruption;
- Ensuring that systems are functioning and faults are reported; and
- Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment

6. **Segregation control.**

Dot maintains industry best practices for separate processing of data collected for different purposes, including:

- Logical segregation of Customer Data;
- Restriction of access to data stored for different purposes according to staff roles and responsibilities;
- Segregation of business information system functions; and
- Segregation of testing and production information system environments.

7. **Risk Management.**

Dot maintains industry best practices for detecting and managing cybersecurity risks, including:

- Threat modeling to document and triage sources of security risk for prioritization and remediation;
- Penetration testing is conducted on the Services at least annually, and any remediation items identified are resolved as soon as possible on a timetable commensurate with the associated risk. Upon request, Dot will provide summary details of the tests performed and whether the identified issues have been resolved;
- Annual engagements of a qualified, independent external auditor to conduct periodic reviews of Dot’s security practices against recognized audit standards, including SOC 2 Type I and SOC 2 Type II certification audits. Upon reasonable request, Dot will provide summary details; and
- A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.

8. **Personnel.**

Dot maintains industry best practices for vetting, training, and managing personnel with respect to security matters, including:

- Background checks, where legally permissible, of employees with access to Customer Data or supporting other aspects of the Services;
- Annual security training for employees, and supplemental security training as appropriate.

9. **Third Party Risk Management.**

Dot maintains industry best practices for managing third party security risks, including with respect to any sub-processor or subcontractor to whom Dot provides Customer Data, including the following measures:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data; and
- Vendor Security Assessments: All third parties undergo a formal vendor assessment process maintained by Dot’s Security team.

10. **Security Incident Response.**

Dot maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data including the following:

- Dot aggregates system logs for security and general observability from a range of systems to facilitate detection and response; and
- If Dot becomes aware that such an event involving Customer Data has occurred, Dot will notify Customer promptly and within the time period required by applicable law.
- Security Evaluations. Dot performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective as measured against industry security standards and its policies and procedures and to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security of Customer Data as well as the maintenance and structure of Dot’s information systems.

Exhibit B
ANNEX II
SUB-PROCESSORS

Snowboard Software GmbH engages certain third-party data processors ('sub-processors') to assist in providing the Snowboard Software GmbH Service. Existing Snowboard Software GmbH sub-processors and the functions they provide are listed below.

SUB-PROCESSORS

Name	Function	Location	Transfer Mechanisms
AWS	Data storage and processing	Chosen by customers	SCCs
Posthog	Product analysis	EU	-
Azure	Data storage and processing	Chosen by customers	SCCs
OpenAI*	Data Processing	US	SCCs

*: If customer decides to go with GPT models hosted on Azure, OpenAI is not a sub-processor anymore.

For all subscribers who have executed Snowboard Software GmbH's DPA, Snowboard Software GmbH will provide advance notice of any proposed updates to the list of sub-processors used. We update this list regularly so that you are informed of the scope of sub-processing associated with the Snowboard Software GmbH Service.