This HOVER Data Processing Agreement (the "**DPA**") is incorporated into the HOVER Terms of Use at https://hover.to/terms-of-use, or applicable governing document (either, the "**Agreement**") and governs HOVER's provision of services as further detailed below. Customer enters into this DPA on behalf of itself, its affiliates, and any entity Customer represents that uses the HOVER services; for clarity, the term "Customer" as used in this DPA shall include Sponsor when applicable. HOVER and Customer are each a "Party" and collectively "the Parties."

This DPA may be updated from time to time with reasonable notice to Customer. Any term not defined in this DPA shall have the meaning set forth in in the Agreement.

1. Definitions. The following definitions apply to this DPA. All capitalized terms of the DPA not defined below shall have the meaning given in the Agreement.

1.1 "**Applicable Law**" includes all laws, regulations and other legal requirements applicable to Customer or HOVER. This may include, for example, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"); equivalent requirements in the United Kingdom including the UK General Data Protection Regulation and the Data Protection Act 2018 ("**UK GDPR**"); the California Consumer Privacy Act and associated regulations ("**CCPA**"), and the California Privacy Rights Act and its implementing related regulations when effective ("**CPRA**"); the Personal Information Protection and Electronic Documents Act, SC 2000, c.5 ("**PIPEDA**"); Australia's Privacy Act 1988 and the Australian Privacy Principles (the "**Privacy Act**"); the Virginia Consumer Data Protection Act when effective ("**VCDPA**"); the Utah Consumer Privacy Act when effective ("**UCPA"**), and the Colorado Privacy Act and related regulations when effective ("**CPA**"). Each party is responsible only for its own obligations under the Applicable Law.

1.2 "Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, imposing notification or other obligations in the event of such a breach.

1.3 "Business" and "Service Provider" have the same meanings as described by Applicable Law.

1.4 "**Controller**" has the same meaning as described by Applicable Law.

1.5 "**Data Subject**" has the meaning as described by Applicable Law.

1.6 "**EEA**" means the European Economic Area, or other adequate country.

1.7 "**Processor**" has the meaning as described by Applicable Law.

1.8 "**Personal Data**" means (i) any information relating to an identified or identifiable individual, within the meaning of the GDPR; (ii) "personal data" within the meaning of the VCDPA and CPA; (iii) "personal information" within the meaning of PIPEDA, the CCPA, the CPRA, and the Privacy Act; and (iv) any analogous term as defined by Applicable Law.

1.9 "**Subprocessor**" means a third party engaged by a Processor for processing Personal Data.

1.10 "**Transfer Mechanism**" means, (i) for the EEA, the Standard Contractual Clauses ("SCC") approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (as amended), (ii) for the UK, the International Data Transfer Agreement ("IDTA") or International Data Transfer Addendum ("IDT Addendum") issued by the Information Commissioner's Office under Section 119A of the Data Protection Act 2018, effective 21 March 2022, or (iii) other recognized compliance standard for lawful data transfers.

1.11 "**UK**" means the United Kingdom.

2. Scope. This DPA applies when use of the HOVER Software and Services involves Personal Data. Customer or HOVER may be a Controller, Processor, or Subprocessor as context requires. Nothing in this DPA restricts Data Subjects from exercising their rights under Applicable Law, including rights to compensation for material and non-material damage in accordance with Article 82 of GDPR or its equivalents under Applicable Law. This DPA does not apply where HOVER and Customer are joint Controllers (in which case HOVER and Customer will execute a separate agreement with respect to processing Personal Data).

3. Parties' obligations.

3.1 Controller instructs Processor to process Personal Data only in accordance with this DPA and only for the purpose of providing the services under the Agreement. Controller is responsible for providing all notices and obtaining all consents, licenses, and legal bases required to allow Processor to process Personal Data. Processor instructs Subprocessor to process Personal Data in accordance with this DPA only for the purpose of providing the services under the Agreement, and is responsible for sharing Controller's instructions with Subprocessor prior to the processing of Personal Data. If HOVER and Customer are independent Controllers, each party agrees to only process Personal Data in accordance with this DPA (unless legally required to do otherwise), to use the technical and organizational measures described in Annex 1 when processing Personal Data, and to provide the other party with reasonable and prompt assistance with responses to data subjects' requests to exercise their rights under the Applicable Laws.

3.2 Processor or Subprocessor will only process Personal Data in accordance with this DPA and Controller's instructions (unless legally required to do otherwise). Processor or Subprocessor will not sell, retain or use any Personal Data for any purpose other than as permitted by this DPA, the HOVER Terms of Use, or HOVER's privacy policy. Processor or Subprocessor will inform Controller immediately if it believes any instructions infringe any Applicable Law. Processor or Subprocessor will use the technical and organizational measures described in Annex 1 when processing Personal Data to ensure a level of security appropriate to the risk involved.

3.3 When required by Applicable Law, Processor or Subprocessor will notify, in accordance with Applicable Law, Controller of any data Breach after becoming aware of the Breach and provide assistance to Controller in accordance with Applicable Laws. Processor or Subprocessor will, without undue delay, provide Controller with reasonable assistance with (i) data protection impact assessments, (ii) responses to Data Subject(s) requests to exercise their rights under Applicable Laws, and (iii) engagement with any appropriate supervisory authority.

3.4 Processor or Subprocessor shall treat Personal Data as confidential information, and will not disclose or use or otherwise process Personal Data except as necessary for HOVER to provide or maintain the services (including internal use as training or research data) or comply with Applicable Law.

3.4.1 Processor or Subprocessor will ensure Personal Data subject to this DPA is only made available to personnel that require access to fulfill the obligations of this DPA, and any such authorized personnel are under obligations of confidentiality to protect and keep the Personal Data in confidence and will only process the Personal Data in accordance with Controller's instructions.

3.4.2 Processor or Subprocessor will provide, if requested by Controller, information or documentation necessary to demonstrate its compliance with confidentiality or other obligations of Applicable Laws or this DPA.

3.4.3 Upon written request, or as required by Applicable Law, Processor or Subprocessor will return or delete any Personal Data in its possession, unless it is legally required to retain it.

3.4.4 If a Data Subject submits a request to Processor or Subprocessor related to Personal Data subject to Controller's instructions, Processor or Subprocessor will promptly forward such request to Controller promptly after Processor or Subprocessor has identified that the request is from a Data Subject for whom Controller is responsible. Controller authorizes on its behalf, and on behalf of its controllers when Controller is acting as a processor, Processor or Subprocessor to respond to any Data Subject confirming the request has been forwarded to Customer. The Parties agree that, when a request is made of HOVER, use of HOVER's privacy web form (available at https://preferences.hover.to/privacy) and HOVER forwarding such data subjects' requests in accordance with this Section, represent the scope and extent of HOVER's required assistance.

3.4.5 In the event Personal Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed, Processor or Subprocessor will inform Controller without undue delay. Processor or Subprocessor will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Personal Data subject to those proceedings is at Controller's disposition.

3.5 Processor or Subprocessor will accommodate Controller's reasonable audit requests, such audits not to occur more than once per year and during normal business hours

except in event of a data Breach. The results of such audit constitute confidential information of the Processor or Subprocessor.

3.6 Controller gives Processor general authorization to engage Subprocessors. Controller may object to a Subprocessor by (i) terminating its relationship with the Processor pursuant to any contractual provisions, (ii) ceasing to use the services the Subprocessor is engaged in, or (iii) requesting the Processor use a different Subprocessor, allowing that the cost of the services may be impacted by fulfilling such request.

3.6.1 Processor will restrict Subprocessor access to Personal Data to only what is necessary to provide the services, and Processor will prohibit the Subprocessor from accessing or using Personal Data for any other purpose.

3.6.2 Processor will enter into a written agreement with its Subprocessors, imposing upon the Subprocessor equivalent obligations to those included in this DPA.

3.6.3 Processor is responsible for compliance with its obligations under this DPA, including any data transfer obligations, and for any act or omissions of its Subprocessors that breach the obligations of this DPA.

3.6.4 Processor may appoint new Subprocessors with reasonable notice to Controller.

3.6.5 HOVER's Subprocessors are listed in Annex 2.

3.7 Data Transfers. HOVER is located in the United States, and Personal Data may be transferred to the United States, pursuant to the terms of any Agreement between HOVER and Customer.

3.7.1 Transfers of Personal Data out of the EEA, UK or other country with data transfer laws will only be made in accordance with the appropriate Transfer Mechanism and this DPA. To the extent required, and provided no alternative Transfer Mechanism is in place, the parties are deemed to have executed the following Transfer Mechanisms by virtue of entering into this DPA:

(i) for transfers out of the EEA, the appropriate SCC module with the following elections:

(a) Clause 7 is not used;

(b) at Clause 9 "General Written Authorization" is provided and the data importer will provide 30 days' advance notice for changes to its list of subprocessors;

(c) the optional language at Clause 11(a) is omitted;

(d) at Clause 17, option 2 is selected and the governing law shall be that of Denmark;

(e) at Clause 18(b) the courts of Denmark shall have jurisdiction

(f) the information at Annex 1 is the information as reflected and supported by the Agreement and this DPA (including any Addendums).

(ii) for transfers out of the UK, the appropriate SCC module as described above is used and supplemented with the ITD Addendum, utilizing the following Mandatory Clauses: "Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO 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."

3.7.2 Subject to the terms of the relevant Transfer Mechanism, if the data importer (as defined by the Transfer Mechanism) receives a request from a governmental body (the "Requesting Party") for access or disclosure of Personal Data, the data importer will use reasonable efforts to direct the Requesting Party to the data exporter (as defined by the Transfer Mechanism).

3.7.3 If compelled to disclose or make available Personal Data to a Requesting Party, the data importer will:

(i) promptly notify the data exporter to allow the opportunity to seek a protective order or other adequate remedy. If the data importer is prohibited from notifying the data exporter of the request, the data importer will use reasonable efforts to obtain a waiver of that prohibition to allow as much communication to the data exporter as possible; and

(ii) challenge any overbroad or inappropriate request (including when such request conflicts with the laws of applicable countries related to the Data Subject(s) involved in such request).

3.7.4 If, after exhausting the steps described in 3.7.3, the data importer remains compelled to disclose Personal Data to the Requesting Party, the data importer will disclose only the minimum amount of Personal Data necessary to satisfy the request and will keep a record of the disclosure.

3.8 Warranty. Processor or Subprocessor agrees and warrants that it has no reason to believe there is legislation applicable to it, or its Subprocessors, including in any country to which Personal Data is transferred either by itself or through a Subprocessor, that prevents it from fulfilling the instructions received from Controller and its obligations under this DPA. In the event of a change in legislation which is likely to have substantial adverse effect on the warranties and obligations provided by this DPA, Processor or Subprocessor will promptly notify the change to Controller as soon as Processor is aware, in which case Controller is entitled to suspend the transfer of Personal Data and/or terminate the Agreement.

4. Entire Agreement; Conflict. Except as supplemented by an addendum to this DPA, the DPA and the Agreement are the final, complete, and exclusive expressions of their terms and

supersede all prior agreements and understandings between the Parties with respect to this subject matter. If there is a conflict between the DPA and one of its addendums, the DPA will control.

GDPR and UK GDPR Addendum to the DPA

This GDPR and UK GDPR Addendum (this "GDPR and UK Addendum") supplements the DPA or Agreement between the Parties governing the processing of Personal Data. This GDPR and UK Addendum applies when the GDPR or UK GDPR applies to HOVER's Software and Services interaction with applicable Personal Data. Unless otherwise defined in this GDPR and UK Addendum, all capitalized terms are defined by the DPA or Agreement.

1. **Processing Controls**. HOVER's privacy request web form (available at https://preferences.hover.to/privacy) may be used to assist the Parties with obligations under the GDPR, including obligations to respond to requests from Data Subjects. Taking into account the nature of the interactions involving the Software and Services, the Parties agree it is unlikely that a Processor or Subprocessor would become aware that Personal Data transferred under a Transfer Mechanism is or would be inaccurate or outdated. Nonetheless, if a Processor or Subprocessor becomes aware that Personal Data transferred under a Transfer Mechanism is inaccurate or outdated, it will inform the Controller without undue delay. Processor will cooperate with Controller to erase or rectify inaccurate or outdated Personal Data transferred under the Transfer Mechanism, such as by responding to appropriate requests received through privacy web forms.

2. **Specified Purpose**. While the Software and Services do not specifically request or require special categories of Personal Information, Controller represents they have obtained necessary and explicit consent for the processing of special categories of Personal Data, for the specified purposes of creating and storing three-dimensional data, rendering, and related data for physical structures, and such other services as described in an Agreement between the Parties from time to time.

3. **Controller Instructions**. The Parties agree that the DPA and the Agreement constitute Controller's documented instructions regarding processing of Personal Data ("Documented Instructions"). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between the Parties, including agreement on any additional fees for carrying out such instructions. Taking into account the nature of the processing, the Parties agree it is unlikely that a Processor or Subprocessor can form an opinion on whether Documented Instructions infringe the GDPR or UK GDPR. If Processor or Subprocessor forms such an opinion, it will inform the Controller, in which case the Controller is entitled to withdraw or modify its Documented Instructions.

CCPA Addendum ("CCPA Terms")

These HOVER CCPA Terms ("CCPA Terms") supplements the DPA and other Agreement between the Parties when the California Consumer Privacy Act of 2018 ("CCPA") or California Privacy Rights Act of 2020 ("CPRA") applies to access, use or otherwise processing of "Personal Information" (as defined and applied in CCPA or CPRA) by the parties. Unless otherwise defined in these CCPA Terms, all capitalized terms are defined by the DPA or Agreement.

The parties each agree and certify, with respect to any Personal Information it receives from the other party under circumstances where the receiving party is acting as a Service Provider, and not already in such receiving party's possession, that it will operate as a Service Provider and will not: (a) retain, use, or disclose Personal Information except as permitted in an agreement between the parties and under CCPA or CPRA, or (b) sell or share Personal Information.

These CCPA Terms do not limit or reduce any other data privacy commitments either party may have under an agreement between the parties.

Switzerland Addendum to the DPA

This Switzerland Addendum (this "Swiss Addendum") supplements the DPA and other Agreement between the Parties governing the processing of Personal Data. This Swiss Addendum applies when the Federal Act on Data Protection ("FADP") applies to HOVER's Software and Services interaction with Swiss Customer Data (as defined below). Unless otherwise defined in this Swiss Addendum, all capitalized terms are defined by the DPA or Agreement.

1. **Applicability**. Except as otherwise set out in this Swiss Addendum, the terms of the DPA will apply to Customer's use of the services to process Swiss Customer Data, and all references to Applicable Law in the DPA will include the FADP, all references to Personal Data in the DPA will include Swiss Customer Data, and all references to "Standard Contractual Clauses" in the DPA will be replaced with "Swiss Standard Contractual Clauses."

2. **Transfers of Swiss Customer Data**. When this Swiss Addendum applies, a Transfer Mechanism includes the Swiss Standard Contractual Clauses to the extent Swiss Customer Data that is transferred, either directly or via onward transfer, to any Swiss Third Country (each a "Swiss Data Transfer"). The Swiss Standard Contractual Clauses will not apply to a Swiss Data Transfer if the Parties have adopted an alternative recognized compliance standard for lawful Swiss Data Transfers pursuant to 1.8(iii) of the DPA.

3. **Definitions**. The following capitalized terms used in this Swiss Addendum have the meaning given to them below:

3.1 "Swiss Standard Contractual Clauses" means the GDPR standard contractual clauses for the transfer of personal data to processors established in third countries with the following modifications:

3.1.1 In instances where the data transfer is subject to both the FADP and the GDPR, the parties adopt the GDPR standard for all data transfers and:

a. The "competent supervisory authority" in Annex I.C under Clause 13 will reflect parallel supervision by the FDPIC.

b. The term "member state" will 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).

c. Protections afforded to data subjects shall include protection for the data of legal entities in accordance with the FADP until the entry into force of the revised FADP.

3.1.2 In instances where the data transfer is exclusively subject to the FADP:

a. The "competent supervisory authority" in Annex I.C under Clause 13 will reflect the FDPIC.

b. The applicable law for contractual claims under Clause 17 will reflect Swiss law.

c. The term “member state” will 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.

d. All references to the GDPR shall be understood as references to the FADP.

e. Protections afforded to data subjects shall include protection for the data of legal entities in accordance with the FADP until the entry into force of the revised FADP.

3.2 “Swiss Customer Data” means the “personal data” (as defined in the FADP) that is uploaded to the Services under Customer’s HOVER accounts. This includes the data of legal entities in accordance with the FADP until the entry into force of the revised FADP.

3.3 “FADP” means the Federal Act on Data Protection of 19 June 1992 until its totally revised version of 25 September 2020 (revised FADP) comes into effect, at which time “FADP” means the revised FADP.

3.4 “FDPIC” means the Federal Data Protection and Information Commissioner.

3.5 “Swiss Third Country” means a country outside Switzerland not recognized by the Secretary of State or the Data Protection Act 2018 as providing an adequate level of protection for personal data (as described in the FADP).

Annex 1 – Processor Security Standards

Processor will undertake and implement the following technical and organizational measures to ensure the security of Personal Data.

1. **Information Security Program**. Processor will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help secure Personal Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to Processor's systems, and (c) minimize security risks, including through risk assessment and regular testing. Processor will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

    1.1 **Network Security**. Processor systems will be electronically accessible to employees, contractors, and any other person as necessary to provide the services. Processor will maintain access controls and policies to manage what access is allowed to Processor systems, including the use of firewalls or functionally equivalent technology and authentication controls. Processor will maintain corrective action and incident response plans to respond to potential security threats.

    1.2 **Physical Security**. Processor represents and warrants it has implemented and maintains the following safeguards. To the extent Processor does not maintain its own physical servers and infrastructure, Processor's cloud infrastructure providers are authorized to provide these same requirements.

        1.2.1 Physical and environmental protection policies, procedures, and systems for Processor systems shall include: emergency lighting, fire protection, temperature and humidity controls, water damage protection, and delivery and removal.

        1.2.2 Physical access to Processor's premises and physical infrastructure, even if hosted by a third party, is protected by physical access authorization, physical access controls and monitoring, and visitor access records to restrict access to authorized personnel only.

2. **Continued Evaluation**. Processor will conduct periodic reviews of the security of its systems and adequacy of its information security program as measured against industry security standards and its own policies and procedures. Processor will continually evaluate the security of its systems and associated services to determine whether additional or different security measures are warranted and to respond to new security risks or findings generated by the periodic reviews.

Annex 2 – The list of HOVER Subprocessors, last updated October 5, 2022 is provided at this link.