DATA PROCESSING AGREEMENT

This Data Processing Addendum, including its Schedules and Appendices, (**"DPA"**) forms part of the Service Agreement or other written or electronic agreement between AllCloud and Customer for the purchase of AllCloud's Services (hereinafter referred to as the **"Services"**) as detailed in the agreement between the parties (the **"Applicable Agreement"**) to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Applicable Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent AllCloud Processes Personal Data for which such Authorized Affiliates qualify as the Controller.

In the course of providing the Services to Customer pursuant to the **Applicable Agreement**, AllCloud may Process Personal Data on behalf of Customer, and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

This DPA covers the Processing of Personal Data by any of AllCloud's Affiliate companies.

1. Definitions

1.1. Capitalized terms used, but not defined, herein shall have the meanings set forth in the applicable data protection law.

1.2. **"Applicable Data Protection Laws"** shall mean: (1) Directive on privacy and electronic communications 2002/58/EC, in as transposed into domestic legislation of each Member State of the European Economic Area and as amended, replaced or superseded from time to time; (2) the EU General Data Protection Regulation2016/679 of the European Parliament and of the Council (**"GDPR"** and collectively with the foregoing **"EU Data Protection Laws"**), any data protection laws substantially amending, replacing or superseding the GDPR following any exit by the United Kingdom from the European Union; (3) the Israeli Protection of Privacy Law, 5741-1981 and any regulations enacted thereunder including the Protection of Privacy (Transfer of Data Abroad) Regulations, 5761-2001 and the Privacy Protection(Data Security) Regulations, 5777-2017, and any guidelines and/or instructions published by the Israeli Privacy Protection Authority; (5) the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., (**"CCPA"**) as modified by the California Privacy Rights Act (**CPRA**) and its implementing regulations (6) and the data protection or privacy laws and regulation of any other country without limitation as may be appliable to the relationship between the parties. No law shall be considered an Applicable Data Protection Law prior to its effective date.

1.3. **"AllCloud's Services"** means AllCloud services as may be published and provided to customers from time to time.

1.4. **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with, the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.5. "**CPRA Addendum**" means the contractual terms required by CPRA when CPRA is applicable to the data being processed.

1.6. **"Customer" –** Any Entity and/or its subsidiaries or affiliates that has a contractual relationship with AllCloud, or is a potential client, to acquire its Services.

1.7. **"Customer Data"-** Any data owned or controlled by the Customer and any data owned or controlled by Customer's prospect, customer, business partners and vendors (i.e., when Customer serves as a Processor to its customers).

1.8. **"EEA Countries"** means countries that are part of the European Economic Area.

1.9. "**Process/Processing**", "**Data Controller**", "**Data Processor**", "**Data Subject**", **"Personal Data"** and "**Special Categories of Personal Data**" shall have the same meaning that such term or substantially equivalent term may be defined in the Applicable Data Protection Laws.

1.10. "**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise Processed by AllCloud and as may be defined by Applicable Data Protection Laws.

1.11. "**Standard Contractual Clauses**" OR "**SCC**" means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR, as adopted by the European Commission Decision 2021/914 of June 4, 2021, which is available at: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.

1.12. "**Swiss Data Protection Laws**" or "**FADP**" means the Swiss Federal Act on Data Protection of June 19, 1992, SR 235.1, and any other applicable data protection or privacy laws of the Swiss Confederation as amended, revised, consolidated, re-enacted or replaced from time to time, to the extent applicable to the processing of Personal Data under the Agreement.

1.13. "**Swiss SCC**" shall mean the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner.

1.14. "**UK Data Protection Laws**" means the Data Protection Act 2018 (DPA 2018), as amended, and the EU General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, as incorporated into UK law as the UK GDPR, and any other applicable UK data protection laws, or regulatory Codes of Conduct or other guidance that may be issued from time to time.

1.15. "**UK GDPR**" means the GDPR as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or a part of the United Kingdom from time to time).

1.16. "**UK SCC**" means the UK 'International data transfer addendum to the European Commission's standard contractual clauses for international data transfers', available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf as adopted, amended or updated by the UK's Information Commissioner's Office, Parliament or Secretary of State.

2. Roles of the Parties.

2.1. The parties acknowledge and agree that, with regard to the Processing of Personal Data, Customer is the Controller, and AllCloud is the Processor. AllCloud will engage Sub-processors pursuant to the requirements set forth in Section 16 "Sub-processors" below.

3. Details of the Processing.

3.1. The subject-matter of Processing of Personal Data by AllCloud is the performance of the Services pursuant to the **Applicable Agreement**. The Customer instructs AllCloud (and authorizes AllCloud to instruct each of its Sub-Processors) to Process the Customer Data, as reasonably necessary for the provision of the Services and in accordance with the **Applicable Agreement** and this DPA.

3.2. The Customer represents and warrants that its Processing instructions shall comply with applicable Data Protection Law and its contractual or legal obligations which relate to the Customer Data concerned. Customer shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Customer acquired the Personal Data. AllCloud shall not be liable for any breach of Customer's contractual or legal obligations towards third parties if it complies with the Applicable Agreement, the terms of this DPA and the applicable laws. AllCloud shall immediately inform the Customer if AllCloud is of the opinion that a Processing instruction received from the Customer infringes Applicable Data Protection Laws and/or is in violation of contractual duties under the Applicable Agreement.

4. Duration of Processing.

4.1. Subject to Section 13 (Deletion and Return) of this DPA, AllCloud will Process Personal Data for the duration of the Applicable Agreement, unless otherwise agreed upon in writing.

5. Categories of Data Subject.

5.1. While performing its Services according to the Applicable Agreement, AllCloud may Process Customer Data that may include, but is not limited to, Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors.
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's end data
- Customer's users authorized by Customer to use the Services.
- Further types of Personal Data that may be Processed by AllCloud are described in AllCloud's Privacy Policy available at https://allcloud.io/full-privacy-policy/ .

6. Type of Personal Data.

6.1. While performing its Services according to the Applicable Agreement, AllCloud may Process Customer Data that may include, but is not limited to, Personal Data relating to the following: First and last name, Title, Position, Employer, Contact information (company, email, phone, physical business address), ID data, Professional life data, Personal life data, Localisation data, Financial Data, Health Data, etc. Further types of Personal Data that may be Processed by AllCloud are described in AllCloud's Privacy Policy available at https://allcloud.io/full-privacy-policy/ .

7. Special Categories of Personal Data.

7.1. Customer shall notify AllCloud prior to the Processing if Customer Data includes special categories of Personal Data, whether any restrictions of Processing apply thereto and whether it has special instruction to adhere with. In the event that there is such Processing: (1) Customer represents that any collection of special categories of Personal Data is subject to specific consent or alternative legal basis as required by the GDPR (where applicable) or according the Applicable Data Protection Laws; (2) AllCloud acknowledges that the access to special categories of Personal Data will be restricted to staff that requires access to carry out their task and who have been informed about the sensitivity of the Processing and the measures to be followed; and (3) the parties acknowledge that special security measures shall be taken when transferring, accessing or storing such data, taking 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 and the transferring shall be under specific consent of the Data Subject.

8. Rights of Data Subjects.

8.1. AllCloud shall, to the extent legally permitted, promptly notify Customer if AllCloud receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Taking into account the nature of the Processing, AllCloud shall assist Customer by appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Applicable Data Protection Laws. In addition, to the extent Customer in its use of the Services does not have the ability to address a Data Subject Request, AllCloud shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent AllCloud is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws. Customer shall be responsible for any costs arising from AllCloud's provision of such assistance.

9. Obligation of Confidentiality.

9.1. AllCloud shall take reasonable steps to ensure the reliability of any employee, agent, contractor, vendor or supplier who may have access Customer Data or Customer's Personal Data, ensuring in each case that access is limited to those individuals who need to know / access the relevant Customer Data and/or Customer Personal Data for the purposes of the Applicable Agreement and to comply with applicable laws, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

9.2. AllCloud shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training regarding their responsibilities and have executed written confidentiality agreements. AllCloud shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

10. Security Measures.

10.1. 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, AllCloud shall, in relation to Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk (collectively, the "**Security Measures**"), including, as appropriate, the following measures:

- Pseudonymisation and encryption of Personal Data;
- Ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- Ability to quickly restore the availability and access to Personal Data in the event ofa physical or technical incident; and
- Maintain a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

10.2. Third-Party Certifications and Audits. AllCloud shall maintain legal, technical and organizational information security measures based on the Israeli Privacy Protection (Data Security) Regulations 5777-2017, the ISO certification mechanisms specified in ISO 27001:2013 – Information Security Management Systems, ISO 27017:2015 – Information Security Controls for Cloud Services. AllCloud shall maintain ISO 27001, 27017 certifications in the scope of Services. Furthermore, AllCloud shall maintain GDPR compliance and undergo annual audit by independent third parties (for GDPR compliance) and the Israeli Standard Institution (for ISO certification).

10.3. Customer agrees that these information security measures are sufficient for its needs or obligations. If additional specific requirements are required by Customer, it will notify AllCloud in writing and will provide it with reasonable time to implement such requirements.

10.4. Customer is obligated to cooperate with AllCloud to use and implement any required Information Security measure delivered to it by AllCloud and according to its instructions, in order to maintain the Security of the data or the security of AllCloud or Customer.

11. Obligation to Notify Data Breaches.

11.1. AllCloud will notify the Customer upon becoming aware (and in no event within more than 72 hours) of any confirmed Security Incident involving the Customer Data in AllCloud's possession or control. AllCloud will provide the Customer with sufficient information, subject to any legal restrictions to which AllCloud is subject, in order to allow the Customer to meet any obligations to report or inform Supervising Authorities and Data Subjects of the Security Incident under Applicable Data Protection Laws, taking into account the nature of Processing and the information available to AllCloud, including a description of the nature of the Security Incident, the categories and approximate number of both Data Subjects and Personal Data records concerned and the likely consequences of the Security Incident.

11.2. Customer's notification regarding a response to a Security Incident under this Section shall not be construed as an acknowledgment by AllCloud of any fault or liability with respect to the Security Incident. AllCloud will, in connection with any Security Incident affecting the Customer Data: (i) quickly and without delay, take such steps as are necessary to contain, remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) co-operate with the Customer and provide the Customer with such assistance and information as it may reasonably require in connection with the containment, investigation, remediation or mitigation of the Security Incident; and (iii) notify the Customer in writing of any request, inspection, audit or investigation by a Supervisory Authority or other governmental authority in connection to the Services where there is not any legal restriction to do so.

12. Assistance with Ensuring Compliance with Art. 32 – 36 GDPR.

12.1. AllCloud shall reasonably assist Customer in ensuring compliance with the obligations pursuant to Art. 32 – 36 GDPR, in particular with respect to the security of the Processing, data protection impact assessments and consultation of supervisory authorities. Upon written request, AllCloud shall provide Customer with the information required for the preparation of the list of Processing operations.

13. Deletion and Return at the End of Processing.

13.1. Upon termination of the Applicable Agreement and/or this DPA, AllCloud will delete or return to the Customer, and instruct its Sub-Processors to delete or return all existing copies of the Customer Data which are in its or its Sub-Processors' possession. Upon written request, AllCloud shall provide written certification to Customer that it has fully complied with the requirements under this Section.

13.2. Notwithstanding the foregoing, AllCloud may retain Customer Data to the extent required by applicable laws to AllCloud and only to the extent and for such period as required by such laws. Furthermore, AllCloud may retain relevant Customer Data solely for the purpose of defending itself against legal claims. Once the legal obligation, or if the legal basis for asserting any legal claim against AllCloud, is no longer in effect, AllCloud shall permanently delete the Customer Data.

13.3. AllCloud shall ensure the strict confidentiality of all such Customer Data, including without limitation, that AllCloud will archive the retained Customer Data in a way that it will only be accessed by specific personnel and only for the reason of archiving it. AllCloud will keep secure the archived data in a level of security which at least is as protective of the Customer's interests as that set forth in this DPA, and all applicable and relevant terms of this DPA and the Applicable Agreement shall remain in effect, for as long as any Customer Data is retained by the Company.

14. Information to Demonstrate Compliance with Data Protection Obligations and Inspections.

14.1. AllCloud shall make available to Customer information (including, for example, copies of its security assessments reflecting controls that have been implemented and relevant security policies) necessary to demonstrate compliance with its obligations under the Applicable Data Protection Laws related to the Applicable Agreement, including its obligations to maintain the security of Personal Data.

15. CROSS-BORDER DATA TRANSFERS.

15.1. If the Processing of Personal Data by AllCloud includes a transfer (either directly or via onward transfer) of such data, the parties agree that the transfer mechanisms listed below shall apply to any transfers of Personal Data under this DPA from the European Union, the European Economic Area ("**EEA**") and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Applicable Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such Applicable Data Protection Laws:

- If, in connection with the Processing of Personal Data originating from the European Union, AllCloud Processes Personal Data outside of the EEA, the parties agree that such transfers shall be subject to the Standard Contractual Clauses for transfer of Personal Data to Processors, with Customer as the "data exporter," and AllCloud as the "data importer" as set forward in **Part 1 of Annex I** ("**EEA Cross Border Transfers**").

- If, in connection with the Processing of Personal Data originating from the UK, AllCloud Processes Personal Data outside of the UK, the parties agree that such transfers shall be subject to the UK SCC, as set forward in **part 2 of Annex I** ("**UK Cross Border Transfers**").

- If, in connection with the Processing of Personal Data originating from Switzerland, AllCloud Processes Customer Data outside of Switzerland, the parties agree that such transfers shall be subject to the Swiss SCC, Subject to the terms set forward in **Part 3 of Annex I** ("**Swiss Cross Border Transfers**").

- The terms set forth in **Annex II (Security Safeguards)** shall apply together with each part of the applicable transfers listed hereabove.

- An approved certification mechanism pursuant to Article 42 or Code of Conduct pursuant to Article 40 of the GDPR together with binding and enforceable commitments of the Processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

15.2. Unless otherwise prohibited in the Applicable Agreement, Customer agrees that in connection with the Services, AllCloud may Process data using one or more of its Affiliate companies meaning that Customer Data may be transferred to countries where an Affiliate company resides. This may include transfers to the following countries: Israel, Canada, Germany, India, Romania and the United States (California, Delaware and New York). All of AllCloud's Affiliate companies are obligated to align with the GDPR standard as relevant to the Processing and are to comply with their Applicable Data Protection Laws.

15.3. Transfer of EEA, UK and Swiss Customer Data to AllCloud's Affiliate companies located in jurisdictions subject to a valid adequacy decision by the competent supervisory authority, including Israel and Canada is allowed on the basis of the applicable adequacy decision.

15.4. Transfers of Customer Data to AllCloud Affiliate companies located in the United States are subject to the Standard Contractual Clauses mechanism of the GDPR, the UK SCC and the Swiss SCC (as applicable) as set out within the data protection agreement between AllCloud Affiliate companies.

16. Sub-processors

16.1. **Appointment of Sub-processors.** The Customer acknowledges that AllCloud may engage Sub- processors to Process the Customer Data for the purpose of providing the Services. The Customer hereby provides general written authorization to AllCloud to engage and appoint such Sub-processors to Process the Customer Data and, subject to the terms of this Section, permits each Sub-processor to appoint a Sub-processor on its behalf. AllCloud has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in the Applicable Agreement and this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

16.2. **List of Current Sub-processors, Notification of New Sub-processors and Objection Right for New Sub-processors**. AllCloud may continue to use those Sub-processors already engaged by AllCloud which may be relevant to perform the Services, and AllCloud may engage an additional or replace an existing Sub-processor to Process the Customer Data, provided that prior to engaging any Sub-processor: (i) it provides a fourteen (14) days' prior written notice to the Customer of its intention to do so, thereby giving the Customer the opportunity to object to such changes on any reasonable grounds by notifying AllCloud promptly in writing within thirty (30) days after receipt of AllCloud's notice. In the event Customer objects to a new Sub-processor, AllCloud will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If AllCloud is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the Applicable Agreement with respect only to those Services which cannot be provided by AllCloud without the use of the objected-to new Sub-processor by providing written notice to AllCloud. Where the Customer objects to the engagement of any Sub-processor, AllCloud shall not transfer the Customer Data to such Sub- processor or otherwise Process the Customer Data through such Sub-processor. Upon the Customer's request, AllCloud shall provide the Customer with an updated list of Sub-processors.

16.3. AllCloud shall, where it engages any Sub-processor (including existing Sub-processors), impose on the Sub-processor, through a legally binding contract between AllCloud and the Sub-processor, data protection obligations no less onerous than those set out in this DPA. Without derogating from the aforesaid, AllCloud shall ensure that such contract will require the Sub-processor to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR and the Applicable Data Protection Laws.

17. Liability.

17.1. Where a Sub-processor fails to fulfil its Personal Data protection obligations with respect to the Customer Data, AllCloud shall remain fully liable to the Customer for the performance of that Sub-processor's obligations.

18. **California Privacy**

18.1. Where CPRA applies, the parties agree to the terms of the CPRA Addendum set forward and attached to this DPA in **Annex III** for the processing of Customer Data subject to CPRA.

19. DPO.

19.1. AllCloud has nominated a Data Protection Officer (DPO) that is responsible and is the primary contact for all AllCloud privacy issues including executing this DPA. The DPO Contact details are:

- Name: Ms. Keren Shtrutzer
- Email: dpo@allcloud.io
- Phone number: +972 (0) 546160634

20. Limitation of Liability.

20.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Applicable Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Applicable Agreement and all DPAs together.

21. Conflict.

21.1. In the event of a conflict between the terms and conditions of this DPA and the Applicable Agreement, this DPA shall prevail. Except as set forth herein, all of the terms and conditions of the Applicable Agreement shall remain in full force and effect.

21.2. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or (ii) if this is not possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.

The parties' authorized signatories have duly executed this DPA:

CUSTOMER	**ALLCLOUD**
Signature:	Signature:
	_____
Customer Legal Name:	AllCloud Legal Name:
Print Name:	Title:

.

Date:

Print Name:

Eran Gil

Title:

CEO

Date:

.

The parties acknowledge that the signatories on their behalf listed above are authorized to sign the name of a party on this DPA.

ANNEX I

CROSS BORDER TRANSFERS

PART 1 – EEA Transfers

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to EEA Cross Border Transfers.
2. Module Two (Controller to Processor) of the SCC shall apply where the EEA Cross Border Transfer is effectuated by the Customer as the data controller of the Personal Data and AllCloud is the data processor of the Personal Data.
3. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.
4. In Clause 9 of the Standard Contractual Clauses - Option 2: GENERAL WRITTEN AUTHORISATION shall apply and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in Section 16 of the DPA.
5. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply.
6. In Clause 17 of the Standard Contractual Clauses, Option 1 shall apply, and the Parties agree that the Standard Contractual Clauses shall be governed by the laws of Germany.
7. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of Germany.
8. Annex I.A of the Standard Contractual Clauses shall be completed as follows:
   8.1. **Data Exporter:** Customer.

   Contact details: As detailed in the Applicable Agreement.

   Data Exporter Role: Module Two: The Data Exporter is a data Controller.

   Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Applicable Agreement.

   8.2. **Data Importer**: AllCloud

   Name (written out in full): AllCloud

   Address: As defined in the Applicable Agreement.

   Contact details: As detailed in the Applicable Agreement.

   Data Importer Role: Module Two: The Data Importer is a Processor.

   Signature and Date: By entering into the Applicable Agreement and / or this DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Applicable Agreement.
9. Annex I.B of the Standard Contractual Clauses shall be completed as follows:
   9.1. The categories of data subjects are described in Section 5 (Categories of Data Subject) of this DPA.
   9.2. The categories of personal data are described in Section 6 (Type of Personal Data) of this DPA.
   9.3. The frequency of the transfer is a continuous basis for the duration of the Applicable Agreement and / or as described in section 4 to this DPA.
   9.4. The nature of the processing is described in Section 3 (Details of Processing) of this DPA.
   9.5. The purpose of the processing is described in Section 3 (Details of Processing) of this DPA.
   9.6. The period for which the personal data will be retained is for the duration of the Applicable Agreement, unless and to the extent agreed otherwise in the Applicable Agreement and/or the DPA.
   9.7. In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth in Section 3 (Details of Processing) of this DPA.
10. Annex I.C of the Standard Contractual Clauses shall be completed as follows:

    The competent supervisory authority in accordance with Clause 13 is The Federal Commissioner for Data Protection and Freedom of Information (BfDI, German: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit).
11. The Security Standards referred to in Annex II of this DPA serve as Annex II of the Standard Contractual Clauses.
12. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses will prevail.

PART 2 – UK Cross Border Transfers

Table 1: The Parties: as stipulated in Section 8 of **Part 1 of this Annex I.**

Table 2: Selected SCCs, Modules and Selected Clauses: as stipulated in **Part 1 of this Annex I.**

Table 3: Appendix Information: means the information which must be provided for the selected modules as set out in the Appendix of the Standard Contractual Clauses (other than the Parties), and which for this Part 2 is set out in **Part 1 of this Annex I**.

Entering into this Part 2:

1. Each Party agrees to be bound by the terms and conditions set out in this Part 2, in exchange for the other Party also agreeing to be bound by this Part 2.
2. Although Annex 1A and Clause 7 of the Standard Contractual Clauses require signatures by the Parties, for the purpose of making UK Transfers, the Parties may enter into this Part 2 in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Part 2. Entering into this Part 2 will have the same effect as signing the Standard Contractual Clauses and any part of the Standard Contractual Clauses.

Interpretation

3. Where this Part 2 uses terms that are defined in the SCCs those terms shall have the same meaning as in the SCCs. In addition, the following terms have the following meanings:

Addendum	This Part 2 which incorporates the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum 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.
Approved EU SCCs	The SCCs
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Part 2 must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Standard Contractual Clauses in any way which is not permitted under the Standard Contractual Clauses or this Part 2, such amendment(s) will not be incorporated by this Part 2 and the equivalent provision of the Standard Contractual Clauses will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Part 2, UK Data Protection Laws apply.

7. If the meaning of this Part 2 is unclear or there is more than one meaning, the meaning that most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted, and/or replaced after this DPA has been entered into.

Hierarchy:

9. Although Clause 5 of Standard Contractual Clauses sets out that the Standard Contractual Clauses prevail over all related agreements between the Parties, the Parties agree that, for a UK Transfer, the hierarchy in Section 9 below will prevail.

10. Where there is any inconsistency or conflict between this Part 2 and the Addendum EU SCCs (as applicable), this Part 2 overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the provisions of this Part 2.

11. Where this Part 2 incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Part 2 impacts those Addendum EU SCCs.

Incorporation and changes to the Standard Contractual Clauses:

12. This Part 2 incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 8 to 10 override Clause 5 (Hierarchy) of the Standard Contractual Clauses; and

    c. this Part 2 (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed on alternative amendments which meet the requirements of Section 11 above, the provisions of Section 14 below will apply.

14. No amendments to the Standard Contractual Clauses other than to meet the requirements of Section 11 above may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12 above) are made:

    a. References to the "Clauses" mean this Part 2, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. To the extent applicable, Clause 8.7(i) of Module One is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules Two and Three is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer; "

    f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

    i. To the extent applicable, the reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module One, is replaced with "Clause 11(c)(i)";

    j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Standard Contractual Clauses do not form part of this Part 2, except for footnotes 8, 9, 10 and 11.

Amendments to this Part 2:

16. The Parties may agree to change Clause 17 and/or 18 of this Part 2 to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Tables 1, 2 or 3 of this Part 2, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised UK Addendum which:

a. makes reasonable and proportionate changes to the UK Addendum, including correcting errors in the UK Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised UK Addendum will specify the start date from which the changes to the UK Addendum are effective and whether the Parties need to review this Part 2 including the Appendix Information. This Part 2 is automatically amended as set out in the revised UK Addendum from the start date specified.

19. If the ICO issues a revised UK Addendum under Section 18, if any Party, will as a direct result of the changes in the UK Addendum have a substantial, disproportionate and demonstrable increase in:

a. its direct costs of performing its obligations under this Part 2; and/or

b. its risk under this Part 2,

and in either case, it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Part 2 at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised UK Addendum.

20. The Parties do not need the consent of any third party to make changes to this Part 2, but any changes must be made in accordance with its terms.

PART 3 – Swiss Cross Border Transfers

The Parties agree that the Standard Contractual Clauses as detailed in Part 1 of this Annex I, shall be adjusted as set out below where the FADP applies to Swiss Transfers:

1. References to the Standard Contractual Clauses mean the Standard Contractual Clauses as amended by this Part 3;

2. The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for Swiss Transfers exclusively subject to the FADP;

3. The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the Standard Contractual Clauses shall be interpreted to include the FADP with respect to Swiss Transfers;

4. References to Regulation (EU) 2018/1725 are removed;

5. Swiss Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named in **Part 1 of this Annex I**;

6. References to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses;

7. Where Swiss Transfers are exclusively subject to the FADP, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP;

8. Where Swiss Transfers are subject to both the FDPA and the GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FDPA insofar as the Swiss Transfers are subject to the

FADP;

9. The Standard Contractual Clauses as amended by this Part 3 also protect the Personal Data of legal entities until the entry into force of the Revised FADP.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

AllCloud shall maintain legal, technical and organizational information security measures based on the Israeli Privacy Protection (Data Security) Regulations 5777-2017, the ISO certification mechanisms specified in ISO 27001:2013 – Information Security Management Systems, ISO 27017:2015 – Information Security Controls for Cloud Services and their respective successors. AllCloud USA shall maintain valid ISO 27001, 27017 certifications. Furthermore, AllCloud is and shall maintain GDPR compliance and undergo annual audit by an independent third party (for GDPR compliance) and the Israeli Standard Institution (for ISO certification).

Data Exporter agrees that AllCloud's maintenance of those minimum information security measures and those described within Section 10 (Security) are sufficient to its needs or obligations. If additional specific requirements are required by data exporter, it will notify data importer, in writing, of such requirements and provide data importer reasonable time to implement such requirements. The data exporter will bear any additional expenses incurred as a result of satisfying such specific requirements. Data importer has the right to reject implementation of the specific security requirement if it has already implemented a substitute or equivalent measure and or, according to its Information Security expert, this measure is not required.

Data exporter is obligated to cooperate with data importer to use and implement any reasonably required Information Security measures or instructions to deliver it as required by the data importer in order to maintain the security of the data or the security of the data importer.

ANNEX III
CPRA ADDENDUM

This CCPA/CPRA Addendum (this "**Addendum**") is incorporated into and forms a part of the DPA and the Applicable Agreement entered into by and between AllCloud ("**Service Provider**") and the Customer (acting as a Business under the CCPA). This Addendum shall be effective the later of: (a) the date You have become a AllCloud Customer (the "**Effective Date**") or (b) January 1, 2023 (CPRA effective date).

If AllCloud receives personal information of California residents from the Customer in order to provide the Services, pursuant to the Applicable Agreements, AllCloud does so as a Service Provider for the purposes of the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 et seq.) as amended by the California Privacy Rights Act ("**CPRA**") (all together herein "**CCPA**") to the extent applicable, and the Customer is a Business.

1. The terms "**Business**", "**Business Purpose**", "**Consumer**" "**Personal Information**," "**Service Provider**," "**Sale**,", "**Sell**" and "**Share**" are as defined in the CCPA. Any capitalized term not defined herein shall have the same meaning ascribed to it in the Applicable Agreement and / or the DPA.

2. AllCloud will not sell or share, as those terms are defined under the CCPA/CPRA, the personal information except as permitted by CPRA.

3. AllCloud will not retain, use, or disclose the personal information for any purpose other than for the business purposes specified in the Applicable Agreement, including but not limited to AllCloud Privacy Policy available at: https://allcloud.io/full-privacy-policy/, including purposes such as retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the Applicable Agreement or as otherwise permitted by CPRA.

4. AllCloud will not retain, use, or disclose the personal information outside of the direct business relationship between Customer and AllCloud or as otherwise permitted by CPRA.

5. Customer agrees that AllCloud may engage other Service Providers and its Affiliates to assist AllCloud in providing the Services to the Customer under the Applicable Agreement. In the event that AllCloud engages a new Service Provider ("Sub-Processor"), AllCloud shall notify Customer of such engagement via the notification mechanism described in section 16 of the DPA.

6. AllCloud will not combine the personal information which it receives from or on behalf of the business, with personal information which AllCloud receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, except as otherwise permitted by CPRA or the regulations adopted by the California Privacy Protection Agency.