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 Customerfor 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 onbehalf of its Authorized Affiliates, if and to the extent AllCloud Processes Personal Data for whichsuch 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 withthe 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

- Capitalized terms used, but not defined, herein shall have the meanings set forth inthe applicable data protection law.
- **"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 orsuperseded 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 theUnited Kingdom from the European Union; (3) the Israeli Protection of Privacy Law, 5741-1981 and any regulations enacted thereunder including the Protection ofPrivacy (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"**) and its implementingregulations (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.
- **"AllCloud's Services"** means AllCloud services as may be published and provided to customers from time to time.

- **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or isunder 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.
- **"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.
- **"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 serve as a Processor to its customers).
- **"EEA Countries"** means countries that are part of the European Economic Area.
- "**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.
- "**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.

2. **Roles of the Parties.** 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 17 "Sub-processors"below.

3. **Details of the Processing.** 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.

3.1. The Customer represents and warrants that its Processing instructions shall comply with applicable Data Protection Law and its contractual or legal obligations whichrelate 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 acquiredthe 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 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**. Subject to Section 13 (Deletion and Return) of this DPA, AllCloud willProcess Personal Data for the duration of the Applicable Agreement, unless otherwise agreedupon in writing.
5. **Categories of Data Subject.** While performing its Services according 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 naturalpersons)
    - Employees or contact persons of Customer's prospects, customers, business partnersand 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**. While performing its Services according 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**. 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 categoriesof Personal Data is subject to specific consent as required by the GDPR (where applicable) oraccording the Applicable Data Protection Laws; (2) AllCloud acknowledges that the access tospecial categories of Personal Data will be restricted to staff that requires access to carry outtheir 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, 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 and the transferring shall be under specific consent of the Data Subject.

8. **Rights of Data Subjects**. 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, forthe fulfilment of Customer's obligation to respond to a Data Subject Request under ApplicableData 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 suchData 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.** AllCloud shall take reasonable steps to ensure the reliability ofany employee, agent, contractor, vendor or supplier who may have access Customer Data orCustomer'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.

9.1. 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.** Taking into account the state of the art, the costs of implementation andthe nature, scope, context and purposes of Processing, as well as the risk of varying likelihoodand 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, asappropriate, 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 effectivenessof technical and organizational measures for ensuring the security of the Processing.

10.1. **Third-Party Certifications and Audits.** AllCloud implements 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 is ISO 27001, 27017 certified. Furthermore, AllCloud is GDPR compliant and is audited annually by independent third parties (for GDPR compliance) and the Israeli Standard Institution (for ISO certification).

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

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

11. **Obligation to Notify Data Breaches.** AllCloud will notify the Customer upon becoming aware(and in no event within more than 72 hours) of any confirmed Security Incident involving theCustomer Data in AllCloud's possession or control. AllCloud will provide the Customer with sufficient information, subject to legal restrictions of AllCloud, to allow AllCloud to meet anyobligations to report or inform Supervising Authorities and Data Subjects of the Security Incident under Applicable Data Protection Laws, taking into account the nature of Processingand 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.

11.1. 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 respectto the Security Incident. AllCloud will, in connection with any Security Incident affecting theCustomer 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 andinformation 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 ofany request, inspection, audit or investigation by a Supervisory Authority or other governmental authority in connection to the Services and where there is not any legal restriction to do so.

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

13.1. 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.

13.2. 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.** 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 GDPR related to the Applicable Agreement, including its obligations to maintain the security of Personal Data.

15. **Disclosure or Publication of Appropriate or Suitable Safeguards for Transfers to a Third Country.** AllCloud makes available the transfer mechanisms listed below which 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:

- The Standard Contractual Clauses (the "SCC Services") set forth in Schedule A to this DPA. In relation to the SCC Services the purpose(s) of the data transfer and further processing is intended to enable the relationship and performance of the Agreement.
- 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 appropriatesafeguards, including as regards data subjects' rights.

15.1. Unless otherwise prohibited in the Applicable Agreement, Customer agrees that in connection with the Services, AllCloud may Process data by one or more of its Affiliate companies meaning that data may be transferred to countries where an Affiliate company resides. This may include the following countries: Israel, Canada, Germany, Romania and theUnited 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.

15.2. Transferring data to AllCloud's Affiliate companies located in Israel and Canada is allowed due to the fact that Israel and Canada are countries that are declared by the EU as countries that have an adequately equivalent level of privacy protection law as to the EU law. The adequacy decision is available for review here: https://ec.europa.eu/info/law/law- topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

15.3. AllCloud Affiliate companies located in the United States are subject to the Standard Contractual Clauses mechanism of the GDPR as set at the Data Protection Applicable Agreement between AllCloud Affiliate companies.

16. **Standard Contractual Clauses.** If, in connection with the Processing of Personal Data originating from the European Union, AllCloud Processes data outside of the European Economic Area, the parties agree to the terms of the Standard Contractual Clauses for Transfer of Personal Data to Processors, with Customer as the "data exporter," and AllCloudas the "data importer." The Clauses are attached hereto as Exhibit A and are incorporated as part of the Applicable Agreement.

17. **Sub-processors**

17.1. **Appointment of Sub-processors.** The Customer acknowledges that AllCloud may engageSub-processors to Process the Customer Data for the purpose of providing the Services. TheCustomer hereby authorizes AllCloud to engage and appoint such Sub-processors to Processthe 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 inthe Applicable Agreement or 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.

17.2. **List of Current Sub-processors, Notification of New Sub-processors and Objection Rightfor 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' priorwritten 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, whichshall 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 Customerobjects 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 anupdated list of Sub-processors.

17.3. 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 requirethe Sub-processor to provide sufficient guarantees to implement appropriate technical andorganizational measures in such a manner that the Processing will meet the requirements ofthe GDPR and the Applicable Data Protection Laws.

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

18. **DPO.** 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 Contactdetails are:

Name: Ms. Admit Ivgi, Legal-Tech Lawyer

Email: dpo@allcloud.io

Phone number: +972(0)546233111

19. **Limitation of Liability.** 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 othertheory 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.

20. **Conflict.** 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 andconditions of the Applicable Agreement shall remain in full force and effect.
21. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPAshall 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:	Print Name:
_____	_Eran Gil_____
Title:	Title:
_____	_CEO_____
Date:	Date:
_____	November 23rd, 2021

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

EXHIBIT A

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified aforesaid in this DPA.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified aforesaid in this DPA.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out specified aforesaid in this DPA, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified aforesaid in this DPA. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described aforesaid in this DPA..

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorization.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract

involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the

applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

SCHEDULE 1

EXHIBIT A

ANNEX I

A. LIST OF PARTIES

Data Importer:	**Data Exporter**:
AllCloud	_____
Name (written out in full): Eran Gil	_____
Position: AllCloud's CEO	_____
Address: As defined in the Applicable Agreement	_____
Signature:_____	**Signature:**_____
Date:_____**November 23rd, 2021**_____	**Date:**_____

B. Categories of data subjects whose personal data is transferred

As states at the DPA.

Categories of personal data transferred

As states at the DPA.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As states at the DPA.

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

As states at the DPA.

Nature of the processing

As states at the DPA.

Purpose(s) of the data transfer and further processing

As states at the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As states at the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As states at the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Federal Commissioner for Data Protection and Freedom of Information (BfDI, German: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)

SCHEDULE 1

EXHIBIT A

ANNEX II

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

AllCloud implements 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 USA is ISO 27001, 27017 certified. Furthermore, AllCloud is GDPR compliant and is audited annually by an independent third party (for GDPR compliance) and the Israeli Standard Institution (for ISO certification).

Data Exporter agrees that those information security measures 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 requirement if it 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 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.