DATA PROCESSING ADDENDUM

Cloud Family AB, or its Affiliates ("**Cloud Family**") and the entity ("**Customer**") using at least one of the Cloud Family Services under the Services Contract (the "**Contract**") entered into between the parties, ("**Cloud Family**" and "**Customer**" respectively or collectively, the "**Parties**"), are agreeing to this Data Processing Addendum ("**DPA**").

1. Definitions

1.1 "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

1.2 **"Data Protection Law**" means, as applicable, any and all applicable domestic and foreign laws, rules, directives, and regulations, on any local, provincial, state or deferral or national level, pertaining to data privacy, data security, and/or the protection of personal data, including the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"), the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**"), Canada Personal Information Protection and Electronic Documents Act 2000 ("**PIPEDA**") the United Kingdom's Data Protection Act 2018 (**"UK-GDPR"**), and the Israeli Protection of Privacy Law, 1981 and the regulations promulgated thereunder ("**PPL**").

1.3 "**Data Subject**" means a data subject to whom personal data relates. Where applicable, Data Subject shall be deemed as a "**Consumer**" as this term is defined under the CCPA.

1.4 **"EEA**" means those countries that are members of the European Economic Area.

1.5 "**Permitted Purposes**" mean any purposes in connection with the Cloud Family performing its obligations under the Contract.

1.6 "**Security Incident**" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. For the avoidance of doubt, any personal data Breach (as defined under the GDPR) will comprise a Security Incident.

1.7 "**Security Measures**" mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of the Cloud Family's business, the level of sensitivity of the data collected, handled, and stored, and the nature of the Cloud Family's business activities.

1.8 "**Standard Contractual Clauses**" shall mean, as relevant, the "Standard Contractual Clauses" under, and as defined by, Regulation EU) 2016/679 of the European Parliament and of the Council has adopted on June 4, 2021, by the European Commission Decision (EU) 2021/914 ("**SCCs**"), attached hereto as Annex 1, as an integral part of this DPA; any standard contractual clauses under the UK GDPR; and any future applicable statutory instruments amending or repealing the above mentioned statutory clauses.

1.9 "**UK GDPR**" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419). Regarding the Standard Contractual Clauses, the applicable process shall be the IDTA Addendum as adopted on February 2, 2022, as detailed under Section 119A of the Data Protection Act 2018 which came into force on March 21, 2022 (as further detailed within Part B to this DPA.

1.10 Sub-Processors

1.11 "**Sub-Processor(s)**" means any Affiliate, agent, contractor or assignee of Cloud Family that may process personal data pursuant to the terms of the Contract, and any unaffiliated processor, vendors, or a service provider engaged by Cloud Family.

1.12 The terms "**controller**", "**processing**" and "**processor**" shall have the meanings ascribed to them in the GDPR, as applicable. Where applicable, a controller shall be deemed to be a "**Business**" under the CCPA, a disclosing "**Organization**" under PIPEDA,, and APA, an "**Owner of a Database**" under the PPL, and a processor shall be deemed to be the "**Service Provider**" under the CCPA, a recipient "**Organization**" under PIPEDA, and APA or a "**Holder of a Database**" under the PPL, respectively, and shall also have the meaning ascribed to equivalent terms under additional applicable Data Protection Laws.

2. Application of this DPA

2.1 This DPA will only apply to the extent all of the following conditions are met:

(A) Cloud Family independently or through the use of Sub-Processors, Processes personal data on behalf of Customer, or on behalf of Customer's applicable client who assume the position of Data Controllers under Data Protection Law, in connection with the Contract;

(B) "processes" (as this term is defined by GDPR and/or by any applicable law or regulation) personal data that is made available by the Customer in connection with the Contract (whether directly by the Customer or indirectly by a third party retained by and operating for the benefit of the Customer);

(C) Data Protection Law applies to the processing of personal data.

2.2 This DPA will only apply to the services for which the Parties agreed to in the Contract and which incorporates this DPA by reference.

3. Parties' Roles

3.1 In respect of the Parties' rights and obligations under this DPA regarding the personal data, the Parties hereby acknowledge and agree that the Customer is the Controller or Processor and Cloud Family is a Processor or Sub-Processor, and accordingly:

(A) Cloud Family agrees that it shall process, either by itself or through its Sub-Processors, all personal data in accordance with its obligations pursuant to this DPA;

(B) The parties acknowledge that the Customer discloses personal data to Cloud Family only for the performance of the Services and that this constitutes a valid business purpose for the processing of such data.

3.2 If Customer is a Processor, Customer warrants to Cloud Family that Customer's instructions and actions with respect to the personal data, including its appointment of Cloud Family as another Processor and concluding the Standard Contractual Clauses, have been authorized by the relevant controller.

3.3 Notwithstanding anything to the contrary in the DPA and Data Protection Laws, Customer acknowledges that Cloud Family shall have the right to collect, use and disclose: (A) data collected in the context of providing the Services, for the purpose of the operation, support or use of its services for its legitimate business purposes, such as account and contract management (including for billing, audit and recordkeeping purposes), technical support, troubleshooting, security, protecting against fraudulent or illegal activity, billing, and for the purpose of establishment/exercise and defense of legal claims; and (B) aggregated and/or anonymized information

4. Compliance with Laws

4.1 Each Party shall comply with its respective obligations under the Data Protection Law.

4.2 Cloud Family shall provide reasonable cooperation and assistance to Customer in relation to Cloud Family's processing of personal data in order to allow Customer to comply with its obligations as a Data Controller under the Data Protection Law.

4.3 The Cloud Family agrees to notify the Customer promptly if it becomes unable to comply with the terms of this DPA and take reasonable and appropriate measures to remedy such non-compliance.

4.4 Throughout the duration of the DPA, the Customer agrees and warrants that:

(A) personal data has been and will continue to be collected, processed, and transferred by Customer in accordance with the relevant provisions of the Data Protection Law;

(B) Customer is solely responsible for determining the lawfulness of the data processing instructions it provides to Cloud Family and shall provide Cloud Family only instructions that are lawful under Data Protection Law;

(C) the processing of personal data by Cloud Family for the Permitted Purposes, as well as any instructions to Cloud Family in connection with the processing of the personal data ("**Processing Instructions**"), has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law; and that

(D) The Customer has informed Data Subjects of the processing and transfer of personal data pursuant to the Contract and this DPA and obtained valid consent or relies on other lawful grounds thereto (including without limitation any consent required by Cloud Family in order to comply with the Processing Instructions and the Permitted Purposes).

5. Processing Purpose and Instructions

5.1 The subject matter of the processing, the nature, and purpose of the processing, the type of personal data and categories of data subjects, and data systems of Customer to which Cloud Family may have access (if any), as applicable, shall be as set out in the Contract, or in the attached Annex 1, which is incorporated herein by reference.

5.2 Cloud Family shall process personal data only for the Permitted Purposes and in accordance with Customer's written Processing Instructions (unless waived in a written requirement), the Contract and the Data Protection Law, unless Cloud Family is otherwise required to do so by law to which it is subject (and in such a case, Cloud Family shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest).

5.3 To the extent that any Processing Instructions may result in the Processing of any personal data outside the scope of the Contract and/or the Permitted Purposes, then such Processing will require a prior written Contract between Cloud Family and Customer, which may include any additional fees that may be payable by Customer to Cloud Family for carrying out such Processing Instructions. Cloud Family shall immediately inform Customer if, in Cloud Family's opinion, an instruction is in violation of Data Protection Law.

5.4 Additional instructions of the Customer outside the scope of the Contract require prior and separate Contract between Customer and Cloud Family, including the Contract on additional fees (if any) payable to Cloud Family for executing such instructions.

5.5 Cloud Family shall not sell, retain, use or disclose the personal data for any purpose other than for the specific purpose of performing the Services or outside of the direct business relationship between the parties, including for a commercial purpose other than providing the Services, except as required under applicable laws, or as otherwise permitted under the CCPA (if applicable) or as may otherwise be permitted for service providers or under a comparable exemption from "sale" in the CCPA (as applicable), as reasonably determined by Cloud Family. The Cloud Family's performance of the Services may include disclosing personal data to Sub-Processors where this is relevant in accordance with this DPA. The Cloud Family certifies that it, and any person receiving access to personal data on its behalf, understand the restrictions contained herein.

6. Reasonable Security and Safeguards

6.1 Cloud Family shall use Security Measures (i) to protect the availability, confidentiality, and integrity of any personal data collected, accessed or processed by Cloud Family in connection with this Contract, and (ii) to protect such data from Security Incidents. Such Security Measures include, without limitation, the security measures set out in Annex 2.

6.2 The Security Measures are subject to technical progress and development and Cloud Family may update or modify the Security Measures from time to time provided that such updates and

modifications do not result in the degradation of the overall security of the services procured by Customer.

6.3 Cloud Family shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who has access to and processes personal data. Cloud Family shall ensure that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.4 Cloud Family is responsible for performing its obligations under the Contract in a manner which enables Cloud Family to comply with Data Protection Law, including implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of personal data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

7. **Security Incidents**

7.1 Upon becoming aware of a Security Incident, Cloud Family will notify Customer without undue delay and will provide information relating to the Security Incident as reasonably requested by Customer. Cloud Family will use reasonable endeavors to assist Customer in mitigating, where possible, the adverse effects of any Security Incident.

8. Security Assessments and Audits

8.1 Cloud Family audits its compliance with data protection and information security standards on a regular basis. Such audits are conducted by Cloud Family's internal audit team or by third party auditors engaged by Cloud Family, and will result in the generation of an audit report ("**Report**"), which will be Cloud Family's confidential information.

8.2 Cloud Family shall, upon reasonable and written notice and subject to obligations of confidentiality, allow its data processing procedures and documentation to be inspected, no more than once a year, by Customer (or its designee), at Customer's expense, in order to ascertain compliance with this DPA. Cloud Family shall cooperate in good faith with audit requests by providing access to relevant knowledgeable personnel and documentation.

8.3 At Customer's written request, and subject to obligations of confidentiality, Cloud Family may satisfy the requirements set out in this section by providing Customer with a copy of the Report so that Customer can reasonably verify Cloud Family's compliance with its obligations under this DPA. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending Cloud Family written notice. If Cloud Family declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Contract.

9. Cooperation and Assistance

9.1 If Cloud Family receives any requests from individuals or applicable data protection authorities relating to the processing of personal data under the Contract, including requests from individuals seeking to exercise their rights under Data Protection Law, Cloud Family will promptly redirect the request to Customer. Cloud Family will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Cloud Family is required to respond to such a request, Cloud Family will promptly notify Customer and provide Customer with a

copy of the request, unless legally prohibited from doing so. The Customer is responsible for verifying that the requestor is the data subject whose information is being sought. Cloud Family bears no responsibility for information provided in good faith to Customer in reliance on this subsection.

9.2 If Cloud Family receives a legally binding request for the disclosure of personal data which is subject to this DPA, Cloud Family shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. It is hereby clarified however that if no such response is received from Customer within three (3) business days (or otherwise any shorter period as dictated by the relevant law or authority), Cloud Family shall be entitled to provide such information.

9.3 Notwithstanding the foregoing, Cloud Family will cooperate with Customer with respect to any action taken by it pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed personal data. Customer shall cover all costs incurred by Cloud Family in connection with its provision of such assistance.

9.4 Upon reasonable notice, Cloud Family shall:

(A) Taking into account the nature of the processing, provide reasonable assistance to the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising Data Subject's rights, at Customer's expense;

(B) Provide reasonable assistance to the Customer in ensuring Customer's compliance with its obligation to carry out data protection impact assessments or prior consultations with data protection authorities with respect to the processing of personal data, provided, however, that if such assistance entails material costs or expenses to Cloud Family, the parties shall first come to an agreement on Customer reimbursing Cloud Family for such costs and expenses.

9.5 Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing Cloud Family to carry out the audit described herein.

9.6 Cloud Family shall appoint a representative as a point of contact and responsible manager for all issues arising out of the Data Protection Laws, who will work together in good faith with the Customer to reach an agreement with regards to any issues arising from time to time in relation to the processing of personal data in connection with this Contract.

10. Use of Sub-Processors

10.1 Customer provides a general authorization to Cloud Family to appoint (and permit each Sub-Processor appointed in accordance with this Clause to appoint) Processors and/or Sub Processors in accordance with this Clause.

10.2 Cloud Family may continue to use those Processors and/or Sub Processors already engaged by Cloud Family as at the date of this Contract, subject to Cloud Family, in each case as soon as practicable, meeting the obligations set out in this Clause.

10.3 Cloud Family can at any time and without justification appoint a new Processor and/or Sub-Processor provided that Customer is given ten (10) days prior notice and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Processor and/or Sub-Processor's non-compliance with Data Protection Law. If, in Cloud Family's reasonable opinion, such objections are legitimate, Cloud Family shall either refrain from using such Processor and/or Sub-Processor in the context of the processing of personal data or shall notify Customer of its intention to continue to use the Processor and/or Sub-Processor. Where Cloud Family notifies Customer of its intention to continue to use the Processor and/or Sub-Processor in these circumstances, Customer may, by providing written notice to Cloud Family, terminate the Contract immediately.

10.4 With respect to each Processor and/or sub-processor, Cloud Family shall ensure that the arrangement between Cloud Family and the Processor and/or Sub Processor is governed by a written contract including terms which offer at least the same level of protection as those set out in this DPA and meet the requirements of Data Protection Law;

10.5 Cloud Family will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Cloud Family to breach any of its obligations under this DPA.

10.6 Cloud Family will only disclose personal data to Sub-Processors for the specific purposes of carrying out the Services on Cloud Family's behalf. Cloud Family does not sell or disclose personal data to third parties for commercial purposes, except as required under applicable laws.

11. Transfer of personal data

11.1 Customer hereby provides Cloud Family with authorization to transfer personal data for the purpose of performing its obligations under the Contract and in accordance with applicable Data Protection Laws.

11.2 EEA/UK/Swiss Data Transfer ("**Cross-Border Transfers**").

11.2.1 Where the processing of personal data includes transfers (either directly or via onward transfer) from the EEA , the UK or Switzerland, outside, respectively, the Parties shall transfer the personal data to an Approved Jurisdiction or be deemed to enter into the Standard Contractual Clauses, including implementing Module 2 (Controller to Processor) between the Parties when necessary, and as referenced in the applicable parts of Schedule 1 of this DPA. Annexes 1-3 attached hereto shall be deemed Annexes 1-3 of the Standard Contractual Clauses as they are referenced in Schedule 1 Part A.

11.2.2 Cloud Family may perform Cross-Border Transfers of personal data provided that the Transfer is necessary for the purpose of Cloud Family carrying out its obligations under the Contract, or is required under applicable laws; and the Transfer is done: (i) to an Approved Jurisdiction, or (ii) subject to appropriate safeguards and Schedule 1 or (iii) in accordance with any of the exceptions listed in the Data Protection Law (in which event Customer will inform Cloud Family in advance which exception applies to each Transfer and will assume complete and sole liability to ensure that the exception applies).

11.3 Canada Transfers.

11.3.1 Where the Cloud Family transfers personal data in or outside of Canada it shall do so only in accordance with the requirements of PIPEDA and applicable laws.

11.4 Transfer outside the State of Israel.

11.4.1 Where the Cloud Family transfers personal data outside of Israel, it shall do so in accordance with the terms of the PPL, including the Protection of Privacy (Transfer of Data to Databases Abroad), 2001.

12. Data Retention and Destruction

12.1 Cloud Family will only retain personal data for the duration of the Contract or as required to perform its obligations under the Contract. Following expiration or termination of the Contract, Cloud Family will delete or return to Customer all personal data in its possession as provided in the Contract and upon request confirm deletion or return in writing, except to the extent Cloud Family is required under applicable laws to retain the personal data. The terms of this DPA will continue to apply to such personal data.

13. General

13.1 Any claims brought under this DPA will be subject to the terms and conditions of the Contract, including the exclusions and limitations set forth in the Contract.

13.2 In the event of a conflict between the Contract (or any document referred to therein) and this DPA, the provisions of this DPA shall prevail.

13.3 Changes. Cloud Family may change this DPA if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the Cloud Family as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party's rights to use or otherwise process personal data; or (iii) have a material adverse impact on Customer, as reasonably determined by Cloud Family.

13.4 Notification of Changes. If Cloud Family intends to change this DPA under this section, and such change will have a material adverse impact on Customer, as reasonably determined by Cloud Family, then Cloud Family will use commercially reasonable efforts to inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

14. **DPA Incorporated By Reference.** This DPA, and all of its terms, are incorporated by reference into, and supplement, the Contract entered into by the Parties, and is effective and binding based upon the Parties' signatures to the Contract.

SCHEDULE 1 – CROSS-BORDER TRANSFERS

PART A: EEA TRANSFERS

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to an EEA Transfer.

2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by the Customer as the data controller of the personal data and Cloud Family is the data processor of the personal data.

3. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.

4. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the Standard Contractual Clauses shall apply, and the method for appointing and time period for prior notice of sub-processor changes shall be as set forth in Section 10.3 of the DPA. Annex 3 lists the sub-processors approved for this engagement as of the signing date of this DPA.

5. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this DPA or the Contract, the provisions of the Standard Contractual Clauses will prevail.

ANNEX 1 TO THE STANDARD CONTRACTUAL CLAUSES – MODULE 2 (CONTROLLER TO PROCESSOR)

The following Annexes form part of the Standard Contractual Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in the following Annexes.

A. List of Parties

DATA EXPORTER (Controller)

Name:	See Contract
Address:	See Contract
Contact person's name, position and contact details:	Signee of Customer
Activities relevant to the data transferred under these Clauses:	Data exporter is a customer of data importer and provides certain personal data to data importer in order to allow data importer to provider services
DPO (if applicable):	N/A
Representative in the EU (if applicable):	N/A

By entering into the Contract 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 Contract.

Signature:	
Date:	

DATA IMPORTER (Processor)

Name:	Cloud Family AB
Address:	Kullaviks korshamnsväg 56, 429 31 Kullavik
Contact person's name, position and contact details:	Henrik Lewander, CTO, henrik.lewander@cloudfamily.com
Activities relevant to the data transferred under these Clauses:	Data importer provides support and services related to Cloud services, and imports certain personal data in order to provide said services
DPO (if applicable):	Henrik Lewander, CTO, henrik.lewander@cloudfamily.com
Representative in the EU (if applicable):	Henrik Lewander, CTO, henrik.lewander@cloudfamily.com

By entering into the Contract and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Contract.

Signature:	
Date:	

B. Description of Transfer

Categories of data subjects whose personal data is transferred:
Customer's personnel who are using the Cloud Family's services.

Categories of personal data transferred:
Credentials of Customer personnel required to sign in to Customer's account, including names, email addresses, and telephone numbers.

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
None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Upon onboarding of Customer's personnel

Nature of the processing:
Storing and accessing credentials in order to allow access to the Cloud Family's Services.

Purpose(s) of the data transfer and further processing:
In order to allow Customer to access the Cloud Family's Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
While each of Customer's personnel has access to the system, as determined by Customer at its sole discretion. All processing will cease upon termination of the underlying Contract or when no longer necessary for the purpose outlined herein.

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

C. Competent Supervisory Authority

The competent supervisory authority regarding this transfer , in accordance with Clause 13 is the

supervisory authority in the Member State stipulated in Annex 1 – EEA Transfers, Section 7 above.

ANNEX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organizational security measures implemented by the data importer in accordance with Clause 8.6 (or document/legislation attached):

TECHNICAL AND ORGANIZATIONAL MEASURES (TOM)

As of: January 2024

The technical and organizational measures are implemented by Cloud Family in accordance with Art 32 of the GDPR. They are continuously improved by Cloud Family according to feasibility and state of the art, not least also in terms of the active ISO 27001 certification and brought to a higher level of security and protection.

1. Confidentiality

1.1. Physical Access Control

Born in the cloud, Cloud Family does not utilize any facilities worldwide.

1.2. Logical Access Control

Measures suitable for preventing data processing systems from being used by unauthorized persons.

Technical Measures	Organizational Measures
✔ Login with username + strong password	✔ User permission management
✔ Anti-Virus Software Clients	✔ Creating user profiles
✔ Firewall	✔ Central password management
✔ Intrusion Detection Systems	✔ Work instruction operational security
✔ Automatic screen lock	✔ Work instruction access control
✔ Encryption of notebooks / tablet	✔ BYOD Device Policy
✔ Two-factor authentication	

1.3. Authorization Control

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Technical Measures		Organizational Measures	
✔	Logging of accesses to applications, specifically when entering, changing, and deleting data	✔	Use of authorization concepts
✔	SSH encrypted access	✔	Minimum number of administrators
✔	Certified SSL encryption	✔	Management of user rights by administrators
		✔	Information Security Policy
		✔	Work instruction communication security
		✔	Work instruction Handling of information and values

1.4. Separation Control

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical Measures		Organizational Measures	
✔	Separation of productive and test environment	✔	Control via authorization concept
✔	Logical separation (systems / databases / data carriers)	✔	Determination of database rights
✔	Multi-tenancy of relevant applications	✔	Information Security Policy
✔	Network segmentation	✔	Data Protection Policy
✔	Client systems logically separated	✔	Work instruction operational security
✔	Staging of development, test and production environment	✔	Work instruction security in software development

1.5. Pseudonymization

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

Technical Measures		Organizational Measures	
✔	In case of pseudonymization: separation of the allocation data and storage in separate system (encrypted)	✔	Internal instruction to pseudonymize personal data as far as possible in the event of disclosure or even after the statutory deletion period has expired
		✔	Information Security Policy
		✔	Data Protection Policy

2. Integrity

2.1. Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Technical Measures		Organizational Measures	
✔	Technical logging of the entry, modification and deletion of data	✔	Information Security Policy
✔	Manual or automated control of the logs	✔	Data Protection Policy

2.2. Input Control

Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical Measures		Organizational Measures	
✔	Technical logging of the entry, modification and deletion of data	✔	Assessment of which programs can be used to enter, change or delete which data

✔	Manual or automated control of the logs	✔	Traceability of data entry, modification and deletion through individual user names
		✔	Assignment of rights to enter, change and delete data on the basis of an authorization concept
		✔	Retention of forms from which data has been transferred to automated processes
		✔	Clear responsibilities for deletions
		✔	Information Security Policy

3. Availability and Resilience

3.1. Availability Control

Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

Technical Measures		Organizational Measures	
✔	Backup monitoring and reporting	✔	BCP policy and procedure
✔	Restorability from automation tools	✔	Control of the backup process
✔	Backup concept according to criticality and customer specifications	✔	Regular testing of data recovery and logging of results
		✔	Storage of backup in a safe place

4. Review, Assessment and Evaluation

4.1. Data Protection Management

Technical Measures		Organizational Measures	
✔	Central documentation of all data protection regulations with access for employees	✔	Internal data protection officer appointed: Group Data Protection Officer (DPO)
✔	Security certification according to ISO 27001	✔	Staff trained and obliged to confidentiality/data secrecy
✔	A review of the effectiveness of the TOMs is carried out at least annually and TOMs are updated	✔	Regular awareness trainings at least annually

✔	Data protection checkpoints consistently implemented in tool-supported risk assessment	✔	Data Protection Impact Assessment (DPIA) is carried out as required
		✔	Processes regarding information obligations according to Art 13 and 14 GDPR established
		✔	Formalized process for requests for information from data subjects is in place
		✔	Data protection aspects established as part of corporate risk management
		✔	ISO 27001 certification of key parts of the company

4.2. Incident Response Management

Support for security breach response and data breach process.

Technical Measures		Organizational Measures	
✔	Use of firewall	✔	Documented process for detecting and reporting security incidents / data breaches (also with regard to reporting obligation to supervisory authority)
✔	Use of phishing, malware attachments, malicious link and spam filter	✔	Formalized procedure for handling security incidents
✔	Use of virus scanner	✔	Documentation of security incidents and data breaches
✔	Intrusion Detection and Prevention Systems	✔	A formal process for following up on security incidents and data breaches

4.3. Data Protection by Design and by Default

Measures pursuant to Art 25 GDPR that comply with the principles of data protection by design and by default.

Technical Measures		Organizational Measures	
✔	No more personal data is collected than is necessary for the respective purpose	✔	Data Protection Policy

✔	Use of data protection-friendly default settings in standard and individual software	✔	Code security checks are performed

4.4. Outsourcing, subcontractors and sub-processing

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Technical Measures		Organizational Measures	
✔	Monitoring of access by external parties	✔	3rd party security assessment and risk analysis as part of the 3rd party acceptance procedure.
✔	Monitoring of subcontractors according to the principles and with the technologies according to the preceding chapters 1, 2	✔	Prior review of the security measures taken by the contractor and their documentation
		✔	Selection of the contractor under due diligence aspects (especially with regard to data protection and data security)
		✔	Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses
		✔	Written instructions to the contractor
		✔	Obligation of the contractor's employees to maintain data security
		✔	Agreement on effective control rights over the contractor
		✔	Data protection policy
			In the case of longer collaboration: ongoing review of the contractor and its level of protection

5. Organization and Data Protection at Cloud Family

In its strategic guideline Quality, Risk and Compliance Policy, Cloud Family has set itself the goal, among other things, of providing its customers with the products and services to be delivered at the highest possible level of information security in compliance with the law. This guideline provides the framework

for transparent, sustainable, process-based and risk-oriented management of the company’s security posture.

In this context, Cloud Family has established a security organization to ensure comprehensive protection of its own information and data protection of its customers' data. The functions of Head of Information Security, Data Protection Officer (DPO), and Legal Compliance Officer (LCO) with group-wide responsibility and direct authority in these areas of activity have been established, and a comprehensive set of internal guidelines and rules have been established, which is binding for all employees and defines secure and data protection-compliant handling of information and data.

Employees are continuously informed and trained in the area of data protection. In addition, all employees are contractually bound to data secrecy and confidentiality. External parties who may come into contact with personal data in the course of their work for Cloud Family are obligated to maintain secrecy and confidentiality as well as to comply with data protection and data secrecy by means of a so-called NDA (Non-Disclosure Agreement) before they begin their work.

Any subcontractors entrusted with further processing (as “other processors”) are only used after approval by the Client as the “controller” and after conclusion of a Data Processing Agreement (DPA) in accordance with Art 28 GDPR, with which they are fully bound by all data protection obligations to which Cloud Family itself is subject.

All of these organizational measures are flanked by Cloud Family's current, high technical security standards, and both dimensions are periodically reviewed and confirmed for adequacy and effectiveness in the course of ongoing internal audits and annually by independent, external, certification bodies as part of the SOC2 and ISO 27001 monitoring and re-certification audits.

ANNEX 3 TO DATA PROCESSING ADDENDUM: LIST OF SUB-PROCESSORS

The table below provides an overview of the third party contractors, who may process our Customer's personal data (sub-processors), to support the provided services.

Sub-processor	Description	HQ Location	GDPR compliance	Point of contact
Technology Providers				
Amazon AWS	Amazon Web Services provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis.	Mountain View, CA	V https://aws.amazon.com/compliance/gdpr-center/	https://aws.amazon.com/privacy (Additional Information for Certain Jurisdictions)
HubSpot, Inc.	HubSpot provides tools for customer relationship management (CRM), social media marketing, lead generation and web analytics. It has TRUSTe certification for Enterprise Privacy and its IT is audited as part of the Sarbanes Oxley compliance. Cloud Family uses HubSpot CRM and analytics tools to manage and automate our sales processes.	Cambridge, MA	V https://legal.hubspot.com/security	privacy@hubspot.com

Part B – UK Transfers - International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: June 4th, 2021

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A above : List of Parties
Annex 1B above: Description of Transfer

Annex 2 above: Technical and organizational measures including technical and organizational measures to ensure the security of the data:
Annex 3 above: List of Sub processors (Modules 2 and 3 only):

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer Exporter neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU 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 Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
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 Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfills the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which 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 Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum 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 Approved Addendum.

11. Where this Addendum 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 Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum 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 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (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 alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

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

a. References to the "Clauses" means this Addendum, 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. Clause 8.7(i) of Module 1 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 2 and 3 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. 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 Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs 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 Part 1: Tables of the Approved Addendum, 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 Approved Addendum which:

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

    b. reflects changes to UK Data Protection Laws;

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

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

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 Addendum 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 Approved Addendum.

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Part C – Switzerland Cross- Border Transfer

The Parties agree that the Standard Contractual Clauses as detailed in Part A of this Schedule 1, shall be adjusted as set out below where the Federal Act on Data Protection of 19 June 1992 (the "**FADP**", and as revised as of 25 September 2020, the "**Revised FADP**") applies to Switzerland Transfers:

1. References to the Standard Contractual Clauses means the Standard Contractual Clauses as amended by this Part C;

2. The Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") shall be the sole Supervisory Authority for Switzerland 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 Switzerland Transfers.

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

5. Switzerland Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named in Part A of this Schedule 1;

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 Switzerland 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 Switzerland Transfers are subject to both the FDPA and the EU GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FDPA insofar as the Switzerland Transfers are subject to the FADP;

9. The Swiss SCCs also protect the Personal Data of legal entities until the entry into force of the Revised FADP.