CUSTOMER DATA PROCESSING ADDENDUM

DoiT International, or its Affiliates ("**Company**") and the entity (“**Customer**”) using at least one of the DoiT International Services under the Services Agreement (the “**Agreement**”) entered into between the parties, ("**Company**" and “**Customer**” respectively or collectively, the “**Parties**”), are agreeing to this Data Protection Addendum (“**DPA**”). This DPA is entered into by Company and Customer and supplements the Agreement. This DPA will be effective and replaces any previously applicable terms relating to its subject matter, from the date of the parties' execution of the Agreement.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

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**") 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 Company performing its obligations under the Agreement.

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 Company’s business, the level of sensitivity of the data collected, handled, and stored, and the nature of the Company’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; EC/2010/87: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council other statutory clauses under Data Protection Laws for the transfer of Personal Data to foreign territories; and any future applicable statutory instruments amending or repealing the above mentioned statutory clauses.

1.9 Processors

1.10 “**Sub-Processor(s)**” means any Affiliate, agent, contractor or assignee of Company that may process Personal Data pursuant to the terms of the Agreement, and any unaffiliated processor, vendors, or a service provider engaged by Company.

1.11 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) Company 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 Agreement;

(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 Agreement (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 Agreement and which incorporates this DPA by reference.

2.3 Customer's contact and billing information are processed by Company in its capacity of a separate and independent Controller and are outside the scope of this DPA.

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 Company is a Processor or Sub-Processor, and accordingly:

(A) Company 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 Company 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 Company that Customer's instructions and actions with respect to the Personal Data, including its appointment of Company 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 Company 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 Company shall provide reasonable cooperation and assistance to Customer in relation to Company'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 Company 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 Company and shall provide Company only instructions that are lawful under Data Protection Law;

(C) the processing of Personal Data by Company for the Permitted Purposes, as well as any instructions to Company 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 Agreement and this DPA and obtained valid consent or relies on other lawful grounds thereto (including without limitation any consent required by Company 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 Company may have access (if any), as applicable, shall be as set out in the Agreement, or in the attached Annex 1, which is incorporated herein by reference.

5.2 Company 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

Agreement and the Data Protection Law, unless Company is otherwise required to do so by law to which it is subject (and in such a case, Company 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 Agreement and/or the Permitted Purposes, then such Processing will require a prior written agreement between Company and Customer, which may include any additional fees that may be payable by Customer to Company for carrying out such Processing Instructions. Company shall immediately inform Customer if, in Company's opinion, an instruction is in violation of Data Protection Law.

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

5.5 Company 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 Company. The Company's performance of the Services may include disclosing Personal Data to Sub-Processors where this is relevant in accordance with this DPA. The Company 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 Company shall use Security Measures (i) to protect the availability, confidentiality, and integrity of any Personal Data collected, accessed or processed by Company in connection with this Agreement, 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 Company 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 Company 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. Company 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 Company is responsible for performing its obligations under the Agreement in a manner which enables Company 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, Company will notify Customer without undue delay and will provide information relating to the Security Incident as reasonably requested by Customer. Company 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 Company audits its compliance with data protection and information security standards on a regular basis. Such audits are conducted by Company's internal audit team or by third party auditors engaged by Company, and will result in the generation of an audit report ("**Report**"), which will be Company's confidential information.

8.2 Company 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. Company 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, Company may satisfy the requirements set out in this section by providing Customer with a copy of the Report so that Customer can reasonably verify Company'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 Company written notice. If Company declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Agreement.

9. Cooperation and Assistance

9.1 If Company receives any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement, including requests from individuals seeking to exercise their rights under Data Protection Law, Company will promptly redirect the request to Customer. Company will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Company is required to respond to such a request, Company 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. Company bears no responsibility for information provided in good faith to Customer in reliance on this subsection.

9.2 If Company receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, Company 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), Company shall be entitled to provide such information.

9.3 Notwithstanding the foregoing, Company 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 Company in connection with its provision of such assistance.

9.4 Upon reasonable notice, Company 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 Company, the parties shall first come to an agreement on Customer reimbursing Company 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 Company to carry out the audit described herein.

9.6 Company 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 Agreement.

10. Use of Sub-Processors

10.1 Customer provides a general authorization to Company 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 Company may continue to use those Processors and/or Sub Processors already engaged by Company as at the date of this Agreement, subject to Company, in each case as soon as practicable, meeting the obligations set out in this Clause.

10.3 Company 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 Company’s reasonable opinion, such objections are legitimate, Company 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 Company 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 Company, terminate the Agreement immediately.

10.4 With respect to each Processor and/or sub-processor, Company shall ensure that the arrangement between Company 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 Company will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Company to breach any of its obligations under this DPA.

10.6 Company will only disclose Personal Data to Sub-Processors for the specific purposes of carrying out the Services on Company's behalf. Company 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 Company with authorization to transfer Personal Data for the purpose of performing its obligations under the Agreement and in accordance with applicable Data Protection Laws.

11.2 EU Data Transfer.

11.2.1 Where the Company transfers Personal Data of residents of the EEA, or to which the GDPR otherwise applies, outside the EEA or an Approved Jurisdiction ("**Transfer(s**)"), the Parties shall be deemed to enter into the Standard Contractual Clauses, implementing Module 2 (Controller to Processor) in which event the Customer shall be deemed as the Data Exporter and the Company shall be deemed as the Data Importer (as these terms are defined therein). Annexes 1-3 attached hereto shall be deemed Annexes 1-3 of the Standard Contractual Clauses.

11.2.2 Company may transfer Personal Data of residents of the EEA outside the EEA provided that the Transfer is necessary for the purpose of Company carrying out its obligations under the Agreement, or is required under applicable laws; and the Transfer is done: (i) to an Approved Jurisdiction, or (ii) subject to appropriate safeguards or (iii) in accordance with any of the exceptions listed in the Data Protection Law (in which event Customer will inform Company 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 Company 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 Company 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 Company will only retain Personal Data for the duration of the Agreement or as required to perform its obligations under the Agreement. Following expiration or termination of the Agreement, Company will delete or return to Customer all Personal Data in its possession as provided in the Agreement and upon request confirm deletion or return in writing, except to the extent Company is required under applicable laws to retain the Personal Data. The terms of this DPA will continue to apply to such Personal Data.

12.2 Notwithstanding the foregoing, Company shall be entitled to maintain Personal Data following the termination of this Agreement for statistical and/or financial purposes provided always that Company maintains such Personal Data on an aggregated basis or otherwise after having removed all personally identifiable attributes from such Personal data.

12.3 Notwithstanding the foregoing, Company shall be entitled to retain Personal Data solely for the establishment or exercise of legal claims, and/or in aggregated and anonymized form, for whatever purpose.

13. General

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

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

13.3 Changes. Company 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 Company 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 Company.

13.4 Notification of Changes. If Company intends to change this DPA under this section, and such change will have a material adverse impact on Customer, as reasonably determined by Company, then Company 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 Agreement entered into by the Parties, and is effective and binding based upon the Parties' signatures to the Agreement.

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:	
Address:	
Contact person's name, position and contact details:	
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):	

Signature:	
Date:	

DATA IMPORTER (Processor)

Name:	DoiT International Ltd
Address:	update accordingly
Contact person's name, position and contact details:	update accordingly
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):	Alex Adler; alexad@doit-intl.com
Representative in the EU (if applicable):	

Signature:	
Date:	

B. Description of Transfer

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

Purpose(s) of the data transfer and further processing
In order to allow Customer to access the Company'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 Agreement 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 is [_________], in accordance with Clause 13.

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: June 2021

The technical and organizational measures are implemented by DoiT International in accordance with Art 32 of the GDPR. They are continuously improved by DoiT International 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, DoiT International 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 DoiT International

In its strategic guideline Quality, Risk and Compliance Policy, DoiT International 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, DoiT International 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 DoiT International 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 DoiT International itself is subject.

All of these organizational measures are flanked by DoiT International'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. Please use the following link to access the latest detailed and up to date list of our sub-processors:

https://help.doit-intl.com/vendor-information/subprocessors

Sub-processor	Description	HQ Location	GDPR compliance	Point of contact
Technology Providers				
Google GCP	Google Cloud Platform provides infrastructure as a service, platform as a service, and serverless computing environments.	Seattle, WA	V https://cloud.google.com/security/gdpr/	https://support.google.com/cloud/contact/dpo
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)
Stripe, Inc.	Stripe offers payment processing and anti-fraud tools which DoiT International uses to accept payments from customers, manage subscriptions, and perform transaction reporting. Stripe is certified as a PCI Level 1 Service Provider, which is the most stringent level of certification available in the payments industry.	San Francisco, CA	V https://stripe.com/guides/general-data-protection-regulation#stripe-and-the-gdpr	dpo@stripe.com
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. DoiT International uses HubSpot CRM and analytics tools to	Cambridge, MA	V https://www.hubspot.com/hubfs/security_documents/HubSpot_Security_Overview.pdf	privacy@hubspot.com

	manage and automate our sales processes.			
Zendesk	Zendesk is a helpdesk software provider. It is compliant with SOC 2/3, ISO 27001 and other security regulations. DoiT International uses Zendesk to accept the customer support tickets, manage and automate the technical support services.	San Francisco, CA	V https://www.zendesk.com/company/privacy-and-data-protection/#gdpr-sub	privacy@zendesk.com
Algolia	The Algolia model provides search as a service, offering web search across a client's website using an externally hosted search engine. Algolia provides their search service via various APIs.The Rest API provides basic features of search, analysis and monitoring.	San Francisco, CA	V https://www.algolia.com/solutions/security/	privacy@algolia.com
Fullstory.com	FullStory is a new kind of platform, designed to help companies answer any question they might have about their digital experience.		V https://help.fullstory.com/hc/en-us/articles/360020623394-GDPR-FAQs	privacy@fullstory.com
Mixpanel	Mixpanel is a business analytics service company. It tracks user interactions with web and mobile applications and provides tools for targeted communication with them. Its toolset contains in-app A/B tests and user survey forms. Data collected is used to build custom reports and measure user engagement and retention.	San Francisco, CA	V https://mixpanel.com/legal/mixpanel-gdpr/	dpo@mixpanel.com
Segment.Io, Inc.	Segment is a popular tool that can be used to collect and send data to various places, including, Zendesk, Optimizely, and one of our favorites, Google Analytics. Segment can be a good option for companies that	San Francisco, CA	V https://segment.com/product/gdpr/	privacy@segment.com

	are sending data to several databases and integrating with lots of different marketing tools.			