Omilia
Conversational Intelligence

Data Processing Addendum (DPA)

1. INTRODUCTION

In addition to those agreed in the Main Contract dated on [Date] between [Full Name and Details of Data Controller] (henceforth referred to as "Data Controller") and [Name of Omilia's Legal Entity], incorporated in [Full Address], [VAT Number/Details], hereinafter referred to as "Omilia", "Data Processor", "Service Provider", jointly referred to as "the Parties" in the Main Contract, the Parties conclude this Data Processing Addendum (DPA) to address data privacy and protection obligations of the Parties in order to comply with various data privacy laws and regulations around the world.

Data Controller enters into this DPA on behalf of itself and in the name and on behalf of its Affiliates, to the extent Omilia processes Customer Data on behalf of such Affiliates as part of the Services. This DPA is presented online and incorporated by the terms and conditions specifically referencing this DPA.

2. SCOPE AND APPLICABILITY

2.1 The provisions of this Addendum apply to all Customer Data, including all records and computational systems used for the processing of Customer Data, with reference to the purposes outlined below (hereafter referred to as "**Processing**").

2.2 The provisions of this Addendum prevail over any other contractual provision already agreed between the Parties in relation to the Processing of Personal Data by Omilia on behalf of Data Controller.

2.3 In order to fulfill its obligations under the Main Contract, Omilia is authorized to conduct, on behalf of Data Controller and on the basis of the provisions of this Addendum, the assigned Data Processing activities referred to in Annex 1.

3. DEFINITIONS

3.1 **In General.** Capitalized terms used in this DPA but not defined herein shall have the meaning given to them in the Main Contract. Other terms not defined herein and related to the protection of personal data, including but not limited to those such as "**consumer**" "**controller**," "**data subject**," "**personal data**," "**personal data breach**," "**processing**," "**processor**," "**sensitive personal data**," "**sell**," "**share**" shall have the meaning assigned to these and materially similar terms (e.g., personal information, (data) breach, etc.) in the Privacy Legislation.

3.2 **Affiliates** means a business entity that: (a) Controls the party; (b) is Controlled by the party; or (c) is under common Control with the party, but only during the time that such Control exists. For the purposes of this definition, "Control(led)" is the ability to determine the management policies of an entity through ownership of a majority of shares or by control of the board of management.

3.3 **Authorities** means any law enforcement agency, government body, regulatory or supervisory authority, court, tribunal, or other public authority with jurisdiction or authority to enforce applicable laws and regulations.

3.4 Customer Data means the personal data that is uploaded to the Service or otherwise disclosed to Omilia by Data Controller or an entity acting on behalf of Data Controller.

3.5 **Data Controller Instructions** means instructions from the entity acting as the Data Controller. The Main Contract as well as this DPA and the instructions provided by Data Controller through its use of the Services shall constitute Data Controller instructions.

3.6 EEA means the European Economic Area.

3.7 **Financial Privacy Legislation** means the Gramm-Leach-Bliley Act ("GLBA") or equivalent state laws such as the California Financial Information Privacy Act ("CalFIPA"), or any regulations promulgated thereunder governing the Processing of NPPI.

3.8 "NPPI" means, as applicable, (i) "non-public personal information" as such term is defined in Regulation P issued by the Consumer Financial Protection Bureau; (ii) "nonpublic personal information" as such term is defined under CalFIPA, and (iii) similar terms as defined under other Privacy Legislation or Financial Privacy Legislation.

3.9 **Privacy Legislation** means any federal, national, state, provincial, regional or local regulation, law, statute, rule or administrative order regulating any processing activities of personal data that is applicable to the parties, as well as any other applicable provisions replacing, supplementing to, or amending, extending, reconstituting, or consolidating them, including without limitation the Financial Privacy Legislation and:

3.9.1 Brazilian Data Protection Law (LGPD), 2018;
3.9.2 Canadian Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5);
3.9.3 EU General Data Protection Regulation 2016/679 (the "GDPR") and the EU Directive on privacy and electronic communications 2002/58/EC;
3.9.4 India's Digital Personal Data Protection Act, 2023, as of date of entry into force, and Information Technology Act, 2011, as applicable.
3.9.5 Mexico's Data Protection Act, 2010;
3.9.6 UK's Data Protection Act 2018, and the GDPR, as incorporated into UK law as the UK GDPR ("UK GDPR");
3.9.7 South Africa's Protection of Personal Information Act (POPIA), 2013;
3.9.8 Swiss Federal Act on Data Protection 235.1 of 25 September 2020, and the Ordinance on the Federal Act on Data Protection 235.11 of 31 August 2022 ("FADP").
3.9.9 United States federal, state, and local data protection laws and regulations, such as the California Consumer Privacy Act of 2018, California Civil Code 1798.100 et seq., as amended from time to time, including by the California Privacy Rights Act of 2020 (together "**US Privacy Legislation**")

3.10 **Service(s)** means the software, cloud services, professional services, and customer care services provided by Omilia to the Data Controller, as further described in the Main Contract.

3.11 **Subprocessor** means any subsequent processor engaged by Omilia, which may include Omilia Affiliates, who agree to process Customer Data on behalf of Omilia.

3.12 Transfer Clauses means any contractual clauses required under Privacy Legislation to transfer personal data from one country to another and that are provided or referenced in Annex [XX] to this DPA.

4. TERM

4.1 The validity of this DPA extends from its signature to any termination of the Main Contract unless otherwise expressly agreed between the Parties.

5. RIGHTS AND OBLIGATIONS

5.1 **Compliance with laws.** Each party will comply with all Privacy Legislation applicable to it. Data Controller shall ensure that all Customer Data disclosed to Omilia has been collected and can be processed through the Services in accordance with the Privacy Legislation, including by providing and collecting any required notices and consents. Where Omilia has any reason to believe that (i) the applicable Privacy Legislation prevents Omilia from fulfilling the Data Controller Instructions and its obligations under this DPA, or (ii) Data Controller Instructions fully or partially infringe the applicable Privacy Legislation, Omilia shall, upon becoming aware of it, promptly inform the Data Controller of such fact, as applicable.

5.2 **Instructions for Data Processing**. Omilia will process Customer Data in compliance with the Data Controller Instructions, this DPA, and the applicable Privacy Legislation. To ensure compliance with its own data protection obligations pursuant to applicable Privacy Legislation, the Data Controller shall independently use the tools and functions provided by Omilia as part of the Services. Only if Data Controller cannot address a requirement under applicable Privacy Legislation with such tools or functions, Data Controller may request reasonable Omilia assistance. The Data Controller will immediately confirm oral instructions in writing. If Data Controller Instructions are given under this DPA, Omilia will document them for the duration of the DPA to ensure the accountability principle of the applicable Privacy Legislation.

5.3 **Sensitive Data**. Data Controller is solely responsible for alerting Omilia in writing as to (i) their use of the Service involving sensitive personal data and/or personal data subject to particular heightened legal requirements, such as under sectoral legislation, and (ii) Data Controller requiring Omilia to apply additional privacy and security measures to such personal data, which are not already included in the Services.

5.4 **Financial Privacy**: Omilia expressly understands and acknowledges that it may have access to, or that Data Controller may disclose to Omilia, NPPI. Without limiting any other obligations in this DPA, Omilia agrees that:

5.4.1 Omilia will use or disclose Data Controller NPPI only as strictly necessary to carry out the purposes for which Data Controller discloses NPPI to Omilia; and
5.4.2 Omilia has implemented and will continue to maintain safeguards reasonably designed to (i) ensure the security and confidentiality of Data Controller NPPI; (ii) protect against any anticipated threats to or hazards to the security or integrity of Data Controller NPPI; and (iii) protect against

unauthorized access to or use of Data Controller NPPI that could result in harm or inconvenience to any individual.

5.5 **Limitations on Processing.** Omilia undertakes to retain, use, process, disclose the Customer Data solely for the specific purposes of performing the Services as specified in Annex 1 and within the contractual scope of the Main Contract, and for no other purpose.

5.5.1 Without limiting the generality of the foregoing, Omilia is prohibited from:

5.5.1.1 Selling or Sharing Customer Data;

5.5.1.2 retaining, using, disclosing, or otherwise Processing Customer Data for any purpose other than for the specific purpose of providing the Services under the Main Contract, including but not limited to (i) marketing or commercially exploiting Customer Data or (ii) disclosing Customer Data for a commercial purpose other than providing the Services specified in the Main Contract;

5.5.1.3 retaining, using, disclosing, or otherwise Processing Customer Data outside of the direct business relationship between Data Controller and Omilia; and

5.5.1.4 combining Personal Data received from or on behalf of the Data Controller with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a Consumer, except where both (i) are expressly required to perform the Services and (ii) are permitted by applicable Privacy Legislation.

5.5.1.5 Omilia hereby certifies that it understands the restrictions set forth in this section and will comply with them.

5.6 Omilia undertakes not to perform any Customer Data Processing activity for its own business purposes, including technical or other testing.

5.7 In the event of any agreement with the Data Controller for the transfer of Personal Data outside the European Union, Omilia undertakes to ensure an adequate level of protection of such data in order to ensure its compliance with the provisions of this DPA.

5.8 **Omilia Personnel**. Omilia personnel may not process Customer Data without proper internal authorization. All Omilia personnel receive data security and privacy training on an annual basis and have agreed to appropriate confidentiality obligations (for the term of their employment and thereafter), insofar as they are not already bound to do so in accordance with relevant legislations and regulations.

5.9 **Security**.

5.9.1 **Technical and Organizational Measures**. Omilia has implemented appropriate technical and organizational measures to maintain and protect the security of its facilities and networks as set forth in Annex 2 to this DPA. The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for Omilia to implement alternative adequate measures, provided such changes do not reduce the security provided. Substantial changes will be documented.

5.9.2 **Review of Omilia Security**. The Data Controller is solely responsible for reviewing the information made available by Omilia relating to data security and making an independent determination as to whether the Services meet the Data Controller requirements as well as applicable Privacy Legislation regarding Customer Data. The Data Controller is solely responsible for ensuring that the Data Controller personnel and consultants follow any end user security guidelines provided by Omilia.

5.10 **Data Subject Rights**. Insofar as a data subject contacts Omilia directly concerning their rights under Privacy Legislation ("Request"), Omilia will promptly notify the Data Controller about such a Request. As part of its Services, Omilia provides tools to the Data Controller to help fulfil such Requests via the Services including, without limitation: [INSERT AS RELEVANT]. If the Customer cannot fulfil such requests using the tools provided on the Services, and insofar as it is included in the scope of Services, Omilia can assist Data Controller without unreasonable delay with the erasure, rectification, data portability and access Requests. Additional Omilia assistance with Request fulfilment will be subject to additional fees at standard rates.

5.11 **Assistance**. To the extent these are not directly available to the Data Controller, Omilia shall, upon request, provide the information, documentation and assistance reasonably necessary for the Data Controller to demonstrate

compliance with the Privacy Legislation requirements. Assistance requested by the Data Controller beyond what is reasonably required under this DPA shall be subject to additional fees at standard rates.

5.12 **Disclosure to Authorities**. Omilia will not disclose Customer Data to Authorities, except as necessary to comply with the law or a valid and binding order (such as a subpoena or a court order). If Authorities request Customer Data from Omilia, it will attempt to redirect the Authorities' request to the Data Controller. As part of this effort, Omelia may provide Authorities with Data Controller contact information. Omilia will promptly notify the Data Controller, if compelled to disclose Customer Data to Authorities unless legally prohibited from doing so.

6. PERSONAL DATA BREACHES

6.1 **Notification and Assistance**. Omilia will notify the Data Controller, as applicable, without undue delay, after becoming aware of a personal data breach. Omilia shall provide details regarding any such personal data breach and continue to provide ongoing communications to the extent this is required for the Data Controller to fulfil its obligations under applicable Privacy Legislation. If required by the applicable Privacy Legislation, Omilia will assist the Company in providing information to the data subject concerned.

6.2 **Mitigation**. Omilia will at its sole discretion take appropriate measures to address the personal data breach and secure any data it processes, as well as its systems and other assets and limit any potential detrimental effects on the data subjects.

7. USAGE OF SUBPROCESSORS

7.1 **Current Subprocessors**. Data Controller authorizes Omilia to disclose Customer Data to Subprocessors, subject to contractual requirements providing personal data protections materially equivalent to those that Omilia has under this DPA, to provide or support the Services and meet other contractual and legal obligations, which have been reviewed by Omilia to ensure the protection of Customer Data, as detailed in the List of Subprocessors Annex [xx] to this DPA.

7.2 **Updates to the List of Subprocessor**s. At least 30 days prior to engaging a new Subprocessor, Omilia will update the List of Subprocessors and notify the Data Controller, as appropriate. Within this period, the Data Controller may object to the new Subprocessor, by contacting [dpo@omilia.com]. The Parties agree to work in good faith to resolve any such reasonable objections raised by the Data Controller. Note that such objections, until resolved, may limit the availability of some features in the Services provided or supported by the Subprocessor(s) in question.

7.3 **Liability for Subprocessor**. Where a Subprocessor fails to fulfil its data protection obligations under this DPA, Omilia shall remain fully liable to the Company for their performance. In any case, Omilia also expressly recognizes its full responsibility towards Data Controller for any act or omission of the subprocessor or any other third party appointed by Omilia as if these were acts or omissions of the same, irrespective of whether the latter complied with its own obligations.

7.4 **Third Party Services**. The Services may function in coordination with various third-party services. If Data Controller uses a third-party service that integrates with Services, Data Controller is solely responsible for ensuring compliance of such third-party services, and that proper data privacy and service terms and conditions, international transfer mechanisms (e.g., customer care, professional services, etc.) are in place with that third-party.

8. AUDITING RIGHT

8.1 Data Controller has the right, at its own expense, to carry out an audit of the performance of the assigned Processing, and in particular of the technical and organizational security measures applied by Omilia, as these measures are specified in this DPA or otherwise agreed between the Parties.

8.2 Data Controller has the right to perform an audit by notifying its intention to Omilia at least thirty (30) days prior to the intended realization, for the purpose of verifying its compliance (and / or its subcontractors) with its obligations arising from the applicable data protection legislation but also from this DPA. Omilia undertakes to provide the Data Controller, at its request, with all the necessary information about its compliance, by providing the appropriate evidence for this purpose.

8.3 This audit is carried out at the discretion of the Data Controller, either by its own or by its specially authorized partners (appropriately bound by confidentiality obligations), once before commencement of the cooperation and then after commencement at regular intervals. The audit may be conducted not more than once a year. The Data Controller bears any and all potential costs involved in the audit.

8.4 For the purpose of this verification, Data Controller has the right to request in particular an on-site inspection at

the Omilia headquarters, at the premises of any subcontractor (sub-executor) of the assigned Processing, or elsewhere the related Processing activities are carried out; other information systems used for the assigned Processing, in relevant records, documents and conventions as reasonably requested by Data Controller within the framework of the aforementioned verification of compliance.

9. INTERNATIONAL DATA TRANSFERS

9.1 Data Controller authorizes Omilia to transfer Customer Data to countries outside of the jurisdiction they originated in, or a jurisdiction that has been found to provide adequate protections under applicable Privacy Legislation, subject to adopting the appropriate safeguards, including Transfer Clauses, as applicable.

9.2 The appropriate Transfer Clauses shall be attached or incorporated in this DPA by reference and apply to any transfers between the parties of Customer Data to countries outside of the jurisdiction they originated in, or a jurisdiction that has been found to provide adequate protections under applicable Privacy Legislation, as applicable.

10. DESIGNATION OF A DATA PROTECTION OFFICER

10.1 Omilia has a Data Protection Officer appointed, whose role is to seek to ensure that the former is in compliance with the applicable data protection legislation and what is predicted in this DPA.

10.2 Omilia undertakes to make available to the Data Controller any audit reports made by the Data Protection Officer and processed by Omilia on behalf of Data Controller pursuant to this DPA.

10.3 Omilia undertakes to promptly correct any data protection defects identified by its Data Protection Officer in the above-mentioned audit reports.

10.4 Omilia undertakes to notify the Data Controller without delay of any changes in personnel that may occur with respect to its Data Protection Officer.

11. COOPERATION WITH THE SUPERVISORY AUTHORITY

11.1 Omilia undertakes (and where required obliges the subprocessors which may be used to undertake the obligation) to cooperate with the competent Supervisory Authority at its request to exercise its powers, including the conduct of investigation and the imposition of penalties or fines.

11.2 In the event that the competent Supervisory Authority conducts audits, inspections, or inquiries of any kind in Data Controller that are directly or indirectly related to the processing activities performed by Omilia on its behalf and which are subject to this DPA, Omilia undertakes to provide appropriate and timely support, as requested by Data Controller.

12. SPECIAL RIGHT OF COMPLAINT

12.1 Data Controller has the right to terminate a part or all of this DPA and / or the Main Contract for a great reason and with immediate effect if Omilia does not comply with its obligations under this DPA. Indicative and non-limiting, non-compliance may refer to any breach of security regulations for information systems, either deliberately or negligently.

12.2 In the case of non-essential derogations or violations, Data Controller undertakes to give Omilia first a reasonable period within which the latter must remedy the deviation or breach.

13. RETURN OF PERSONAL DATA

13.1 At the sole discretion of Data Controller, Omilia undertakes to return or delete all Personal Data inside or outside of its own premises or its subcontractors', including electronic copies on primary and secondary servers, upon receipt of a request from Data Controller and in any case after the termination in any way of the Main Contract, or otherwise completing the assigned Processing.

13.2 In the event that Data Controller is required to irreversibly destroy or delete the Personal Data of the assigned Processing, as they are in any form of documents and / or other recipients of data, Omilia undertakes to provide a written assurance that irreparable destruction or deletion, in accordance with applicable standards and any specific procedures ordered by Data Controller.

14. FINAL PROVISIONS

14.1 **Entire Agreement.** This DPA and the Main Contract, as well as any subsequent Annex agreed by the Parties, constitutes the entire agreement on the protection of personal data and replaces any previous agreement, contract, negotiation, and discussion with each other on this matter.

14.2 The provisions of this DPA are agreed in the interest of the Parties and are fully binding to them, as well as any corresponding successors and assignees.

14.3 **Conflicts**. Except as amended by this DPA, the Main Contract will remain in full force and effect. If there is a conflict between the Main Contract and this DPA, the terms of this DPA will control. If there is a conflict between the Main Contract, this DPA, and Transfer Clauses, the Transfer Clauses shall control.

14.4 **Amendment.** Any amendment to this DPA shall be made in writing and only upon written declaration of mutual agreement between the Parties.

14.5 **Severability** In the event that one or more of the provisions of this DPA becomes void or incomplete in whole or in part, it is expressly agreed by the Parties that this does not affect the validity of the other provisions.

15. LIABILITY AND INDEMNIFICATION, NOTICES, GOVERNING LAW AND JURISDICTION

15.1 Parties agree that any limitations of liability, liability disclaimers, indemnifications, notice requirements, governing law and jurisdiction clauses contained in the Main Contract shall equally apply under this DPA.

ANNEXES

Annex 1 – Data Processing Description
Annex 2 – Subprocessors
Annex 3 – Technical and Organizational Measures

Annex 4 –Transfer Clauses
Annex 4a – EEA Transfer Clauses
Annex 4b – UK Transfer Clauses
Annex 4c – Swiss Transfer Clauses

THE PARTIES

FOR OMILIA		FOR DATA CONTROLLER	
[Name of Omilia's Legal Entity]		**[Data Controller Name]**	
Signature:		Signature:	
Name:		Name:	
Title:		Title:	
Date:		Date:	

Omilia
Conversational Intelligence

Annex 1

Schedule to Data Processing Addendum as of [Date]

1. DESCRIPTION OF PROCESSING ACTIVITY

The Data Processor, in the context of the cooperation between the Parties for the provision of services, acquires access to and/ or receives the Personal Data from the Data Controller in order to process them exclusively for the execution of the Main Contract and provision of Services to the Data Controller. The Data Processor maintains processing in strict compliance with this Schedule, Data Processing Addendum and the Main Contract as well as guidance, instructions and requirements of the Data Controller.

2. CATEGORIES OF PERSONAL DATA TO BE PROCESSED

☐ ***Data Controller's details*** (name, registered address, telephone and mobile numbers, email addresses, name of contact person, his/her date of birth, gender, service use history and details, authentication and authorization details)
☐ ***Data Controller's customers' details*** (name, title, home address, telephone and mobile numbers, email address, date of birth, gender, customer number, purchase and/or service use history and details, authentication and authorization details)
☐ ***Financial and transactional details*** (payments, items purchased, bank account number, payment transaction information, credit card number/ pin/ ccv/ expiration date)
☐ ***Health information*** (credit card number and common medical condition; credit card number and sensitive disease or drug; medical imaging files; DNA profile; name and date of birth; ICD9 code and description; ICD9 code and name; ICD9 description and name; ICD10 code and description; ICD10 code and name; ICD10 description and name; medical form information; name and common medical condition; name and contact information; name and health insurance claim numbers (HICN); name and Medicare Beneficiary Identifiers (MBI); name and sensitive disease or drug; national drug code (NDC) number; SPSS text files; SSN and common medical condition; SSN and sensitive disease or drug; insurance contract details, insurance coverage, insurance payments, beneficiaries, insurance history)
☐ ***IT management details*** (details of equipment data related to the services provided including technical identifiers, username, location, contact details, communication data and metadata and technical events related to the services provided including system and application logs)
☐ ***Security details*** (security log information, security incident information)
☐ ***Personal data*** (name, address, location, online identifier, income)
☐ ***Other*** (any other data provided by the Data Controller/ Data Subject to the Data Processor for the purpose of executing the Main Contract and/ or provision of the Services under the Main Contract).

3. SPECIAL CATEGORIES OF DATA TO BE PROCESSED ALONG WITH SAFEGUARDS AND RESTRICTIONS FOR THEIR PROCESSING (IF APPLICABLE)

a. Special categories of data

☐ **Health information**
☐ **Financial and transactional details**
☐ **Other (specify):** [please complete accordingly]

b. Safeguards and restrictions the Data Processor applies for processing of sensitive data:

- strict purpose limitation,
- access restrictions (including access only for staff having followed specialized training),
- keeping a record of access to the data,
- prohibition of onward transfers of sensitive data,
- encrypted communication channels (data in transit),
- encrypted storage (data at rest),
- data leakage protection / prevention mechanisms,

- physical secure working environment.

4. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS PROCESSED

Direct customers and clients of the Data Controller (End Users).

5. NATURE OF PROCESSING

collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

6. PURPOSE OF PROCESSING

To provide the Services as agreed in the Main Contract

7. DURATION AND FREQUENCY OF PROCESSING (AD-HOC OR CONTINUOUS PROCESSING)

Continuous

8. DURATION OF RETENTION OF THE DATA AND PROCEDURE FOR ITS DELETION

The duration of the Main Contract and for the term imposed or permitted by applicable law.

9. SUB-PROCESSING

The Data Processor may engage affiliated companies and/ or its contractors, subject to the requirements of the Data Processing Schedule, which include the conclusion of EU Standard Contractual Clauses for transfers outside the European Economic Area.

10. DATA TRANSFERS

The Data Processor is authorized, in connection with the provision of the Services, or in the normal course of business, to make worldwide transfers of Personal Data to its affiliates and/or Subprocessors.

When making such transfers, the Data Processor shall ensure appropriate protection is in place to safeguard the Personal Data transferred under or in connection with this Agreement. Where the provision of Services involves the transfer of Personal Data from the European Economic Areas ("EEA") to countries outside the EEA (which are not subject to an adequacy decision under Privacy Laws), such transfer shall be subject to the following requirements: (a) the Data Processor has in place intra-group agreements with its affiliates and contractors which may have access to the Personal Data, (b) the Data Processor has in place agreements with its Subprocessors that incorporate the relevant Clauses as appropriate.

Annex 2 – Subprocessors

Omilia may disclose Company personal data to Subprocessors listed on the following website (along with their subsidiary companies), depending on what Services, features and functionality Data Controller decides to use. Omilia may use its Affiliates as Subprocessors to provide support and troubleshooting, depending on the region Data Controller is based in.

Data Controller acknowledges that changes to this website shall constitute notice of changes to Subprocessors.

Omilia
Conversational Intelligence

ANNEX 3: TECHNICAL AND ORGANIZATIONAL MEASURES ADOPTED TO ENSURE THE SECURITY OF DATA

Cybersecurity Introduction and Relevant Definitions

Omilia has implemented and maintains appropriate physical, organizational and technical safeguards to ensure a level of security appropriate to the risk designed to protect Customer Data and provide ongoing confidentiality, integrity, and availability of Processing systems and services. In the sections below, the following definitions apply:

"**Cybersecurity**" shall mean the act of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. This includes Information Technology security and information security.

"Omilia Systems" refers to Omilia systems that connect to Data Controller's systems, which are a part of Omilia's services to Data Controller, which are critical to Data Controller operations, or that process or store Customer Data.

Omilia has implemented the following technical and organizational safeguards:

1. Access Control:

   a. Preventing Unauthorized Access

      i. Physical access: Physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.

      ii. Remote Access: Remote access to Omilia infrastructure for internal users is controlled using Multi Factor Authentication (MFA) and/or a Virtual Private Network (VPN), subject to password security settings.

      iii. Authentication: A unique account and password are required to authenticate users in Omilia Systems.

      iv. Authorization: Omilia's access controls are designed to ensure that only the appropriately assigned individuals can access specific systems or data. Authorization to Customer Data is performed through validating the user's permissions against the attributes associated with the system or environment housing Customer Data.

   b. Preventing Unauthorized Product Use

      i. Access controls: Omilia has implemented Network access control mechanisms that are designed to prevent network traffic using unauthorized protocols from reaching Omilia Systems. The technical measures implemented differ between system infrastructure providers and include security group assignment and firewall rules.

      ii. Intrusion detection and prevention: Omilia has implemented a Web Application Firewall (WAF) solution to protect boundaries within the application as well as and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

      iii. Dynamic application security testing: Omilia performs internal vulnerability scans on the Omilia Systems to identify critical threats and security weaknesses. Findings from the scanning are analyzed and prioritized. Vulnerabilities and threats are addressed within reasonable timeframes that align with industry standards.

      iv. Penetration testing: Omilia maintains relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios as well as receiving receive a risk score based on the third-party analysis/penetration test.

   c. Limitations of Privilege & Authorization Requirements

      i. A limited number of Omilia's employees have access to Customer Data. All permission elevation requests are logged. Employees are granted access by role, and reviews of elevated privilege grants are initiated regularly.

ii. Omilia undertakes employee onboarding process and background checks in certain jurisdictions. Omilia includes the employee privacy and security awareness training in the Omilia onboarding process and regular employee training.

2. Data Encryption

a. Omilia uses HTTPS encryption (TLS 1.2 or more recent) to protect data in transit.

b. Omilia uses an industry standard AES-256 encryption algorithm to protect data at rest.

3. Detection and Response

a. Detection: Omilia Systems are designed to log information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Omilia personnel, including security, operations, and support personnel, are responsive to known incidents.

b. Response and tracking: Omilia maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented.

4. Availability Control

a. Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure.

b. A disaster recovery policy is in place and is reviewed on an annual basis. Disaster recovery testing is performed at least annually. Key stakeholders are involved in the planning, execution, and remediation (if required).

c. Business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

Annex 4 –Transfer Clauses

To give effect to the requirements in Section 11 of this DPA, parties attach and where possible incorporate by reference the following Transfer Clauses, which have been divided by jurisdiction in Annexes 4a et seq., as applicable.

Annex 4a – EEA Transfer Clauses

1. APPLICABILITY.

a. Transfers among Parties. When the parties transfer among themselves Customer Data, which is subject to the GDPR or EEA Transfer Clauses by virtue of a transfer, to a non-EEA country, which has not been found to provide adequate protections to personal data by relevant Authorities ("Third Country"), Parties agree to and incorporate by reference to this DPA, an appropriate module of the standard contractual clauses set out in the Annex to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time ("EEA Transfer Clauses"), depending on whether they act in their capacity as a controller or processor, as outlined in Section 2 of this DPA.

b. Omilia Transfers to Subprocessors. When Omilia shares Customer Data, which is subject to the GDPR or EEA Transfer Clauses by virtue of an onward transfer with a Subprocessor in a Third Country, they shall conclude Module three of the EEA Transfer Clauses.

c. Data Importer and Data Exporter. For the purposes of the EEA Transfer Clauses, the party transferring Customer Data subject to the GDPR is the "data exporter" and the party receiving Customer Data in the Third Country is the "data importer".

2. EEA TRANSFER CLAUSES MODULES.

a. Controller-to-Processor. The module two: Transfers Controller to Processor of the EEA Transfer Clauses shall be deemed completed as follows:

i. Optional Clause 7 ("Docking clause") shall be deemed incorporated.

ii. In Clause 9(a) ("Use of sub-processors"), the Parties choose Option 2, 'General Written Authorisation', with a time period subject to Section 3.k.ii. of the DPA.

iii. In Clause 11(a) ("Redress"), optional wording shall not be deemed incorporated.

iv. In Clause 17 ("Governing law"), Parties choose Option 1, and agree that EEA Transfer Clauses shall be governed by the law of the EEA Member State where the data exporter is established.

v. In Clause 18 ("Choice of forum and jurisdiction"), the Parties agree that any disputes arising from EEA Transfer Clauses shall be resolved by the courts of the EEA Member State where the data exporter is established.

vi. Annex I.A ("List of parties") and I.B ("Description of transfer") shall be deemed completed with the information set out in Section 1.c. of this Annex 4a and in the Annex 1 to this DPA.

vii. Annex I.B ("Description of transfer") shall be deemed completed with the information set out in Annex 1 to this DPA.

viii. For the purpose of Annex I.C ("Competent supervisory authority"), the competent supervisory authority in the EEA Member State where the data exporter is established.

ix. If the data exporter is not established in the EEA and personal data sharing under this DPA is subject to the EEA Transfer Clauses by virtue of the extraterritorial application of the GDPR, or an onward transfer, the 1) applicable governing law under Section 2.a.iv.; 2) courts under Section 2.a.v.; and 3) competent authority under Section 2.a.viii of this Annex 4a to the DPA shall be those of the EEA Member State identified in the original EEA Transfer Clauses which the data exporter is subject to. Data exporter shall notify data importer of such EEA Member State upon request.

x. Annex II ("Technical and organizational measures") shall be deemed completed with the information set out in Annex 3 to this DPA.

xi. Annex III ("List of sub-processors") shall be deemed completed with the information set out in Annex 2 to this DPA.

Annex 4b – UK Transfer Clauses

1. APPLICABILITY.

a. Transfers among Parties. When the parties transfer among themselves Customer Data, which is subject to the UK GDPR or UK Transfer Clauses by virtue of an transfer, to a Third Country, Parties agree to and incorporate by reference to this DPA the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force 21 March 2022, and as may be amended or replaced by the UK Information Commissioner's Office and approved by UK Parliament, or/and the Secretary of State from time to time ("UK Transfer Clauses"), incorporating the appropriate EEA Transfer Clauses modules, depending on whether they act in their capacity as a controller or processor, as outlined in Section 2 of this DPA.

b. Omilia Transfers to Subprocessors. When Omilia shares Customer Data, which is subject to the UK GDPR or UK Transfer Clauses by virtue of an onward transfer with a Subprocessor in a Third Country, they shall conclude UK Transfer Clauses incorporating module three of the EEA Transfer Clauses.

c. Data Importer and Data Exporter. For the purposes of the UK Transfer Clauses, the party transferring Customer Data subject to the UK GDPR is the "data exporter" and the party receiving Customer Data in the Third Country is the "data importer".

2. UK TRANSFER CLAUSES.

a. Completion. UK Transfer Clauses shall be deemed completed as follows:

i. Table 1 shall be deemed completed with the relevant information set out in Section 1.c. of Annex 4a and in the Annex 1 to this DPA;

ii. In Table 2, the Parties select the checkbox that reads: "The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information", and for this purpose, the Parties hereby agree to apply the content of the appropriate module(s) of EEA Transfer Clauses, as set out in Annex 4a to this DPA;

iii. Table 3 shall be deemed completed with the relevant information applicable to the appropriate module(s) of EEA Transfer Clauses incorporated into the UK Transfer Clauses, as set out in Annex 4a to this DPA (including any cross-references to other Annexes it may contain);

iv. The Parties agree that both Parties may end the UK Transfer Clauses as set out in Section 19 of the UK Transfer Clauses.

Annex 4c – Swiss Transfer Clauses

1. APPLICABILITY.

a. Transfers among Parties. When the parties transfer among themselves Customer Data, which is subject to the FADP, to a Third Country, Parties agree to and incorporate by reference to this DPA the appropriate modules of the EEA Transfer Clauses adapted for the use under the FADP, as outlined in Section 2 of this Annex 4c to the DPA("Swiss Transfer Clauses"), depending on whether they act in their capacity as a controller or processor, as outlined in Section 2 of this DPA.

b. Omilia Transfers to Subprocessors. When Omilia shares Customer Data, which is subject to the FADP with a Subprocessor in a Third Country, they shall conclude module three of the Swiss Transfer Clauses.

c. Data Importer and Data Exporter. For the purposes of the Swiss Transfer Clauses, the party transferring Customer Data subject to the FADP is the "data exporter" and the party receiving Customer Data in the Third Country is the "data importer".

2. SWISS TRANSFER CLAUSES.

a. Completion. Swiss Transfer Clauses shall be deemed completed as follows:

i. Swiss Transfer Clauses shall be completed as outlined in Section 2. of the Annex 4a, as applicable, subject to the below changes.

ii. The term 'member state', as used in the EEA Transfer Clauses, must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility bring proceedings regarding their rights against the data importer and/or data exporter in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EEA Transfer Clauses.

iii. With regards to Annex I.C to the EEA Transfer Clauses, Swiss Federal Data Protection and Information Commissioner (the "FDPIC") shall (also) be the competent Supervisory Authority, as follows. When transfer is subject to both the FADP and the GDPR, parallel supervision should apply (i.e., FDPIC shall be competent insofar as the Customer Data transfer is governed by the FADP; competent EEA Authority shall be competent insofar as the Customer Data transfer is governed by the GDPR). Where transfer is subject exclusively to the FADP, the competent supervisory authority is the FDPIC.

iv. With regards to Clause 17 of the EEA Transfer Clauses, the governing law for contractual claims shall be the law of Switzerland or the EEA Member State where the data exporter is established.

v. With regards to Clause 18b of the EEA Transfer Clauses, the place of jurisdiction for actions between the parties shall be the Swiss courts or the courts of the EEA Member State where the data exporter is established.

vi. References to the GDPR should be understood as references to the FADP, as applicable.