DATA PROCESSING AGREEMENT
INFINNI INNOVATIONS, S.A.

This Data Processing Agreement, including its Appendix ("**DPA**"), forms part of the INFINNI's Terms of Service or other written or electronic agreement between INFINNI and Customer for the purchase of services (the "**Agreement**").

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

HOW TO EXECUTE THIS DPA

1. This DPA consists of the main body and its Annexes, and Appendix I and its Annexes if international data transfers are carried out.

2. This DPA has been pre-signed on behalf of INFINNI in Annex I of the Standard Contractual Clauses ("**SCCs**") between controllers and processors under Article 28(7) set out below.

3. To complete this DPA, Customer must:

    a. Complete the information requested in **Annex I** to the SCCs between controllers and processors under Article 28(7) of the GDPR included below and sign it.

    b. Send the signed DPA to INFINNI by **email to dpo@infinni.io**, indicating the Customer's account or agreement reference where applicable.

    c. In the event that the processing implies carrying out international transfer of personal data, the Customer must inform INFINNI of this fact in the email sent to it and complete, sign and send **Annexes I and II to Appendix I** where the SCCs for international data transfers are included [incorporating Module 3 (Processor to Processor) and Module 4 (Processor to Controller)]. With the signing of these Annexes, the Customer accepts such clauses as safeguards to govern the international transfers of personal data carried out under this DPA.

This DPA becomes legally binding upon receipt by INFINNI of the validly completed and signed DPA (and, if applicable, Appendix I) at the above address. However, INFINNI shall review its content and, in the event that the Customer has not complied with the instructions provided under this DPA for its completion, has included changes not permitted under such instructions or has modified the SCCs and / or other clauses, INFINNI may propose the necessary amendments to reach an agreement, which the Customer and INFINNI shall discuss in good faith.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. The INFINNI entity party to the Agreement is party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and not legally binding. Such entity should request that the contracting Customer entity executes this DPA.

DATA PROCESSING AGREEMENT (DPA)

The European Commission adopted, by means of Commission Implementing Decision (EU) 2021/915 of 4 June 2021, standard contractual clauses between controllers and processors referred to in Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter, "**GDPR**") a set of SCCs for the formalization of the relationship between data controllers and processors. To comply with Article 28 of the GDPR, the Parties agree to execute the SCCs adopted by the European Commission which are set out below.

I. Roles of the Parties

The Customer may act as data controller or as data processor and INFINNI as data processor (when the Customer acts as data controller) or (sub)processor (when the Customer acts as data processor), as identified for this specific relationship in **Annex I** of the SCCs between controllers and processors under Article 28(7) of the GDPR set out below.

For the purposes of the proper application of this DPA in both of its intended use cases, the Parties hereby agree to the following rules of interpretation:

1. **Scenario 1**: Use as a **Data** Controller – **Data** Processor Agreement. Where this DPA is entered into or applied to govern the relationship between a data controller (Customer) and a data processor (INFINNI), all references in the SCCs to the "controller" and to the "processor" shall be construed in their literal sense, in accordance with the definitions set forth in Article 4(7) and Article 4(8) of the GDPR, respectively.

2. **Scenario 2**: Use as a **Data** Processor – **Data** Sub-processor Agreement. Where this DPA is entered into or applied to govern the relationship between a data processor (Customer) and a sub-processor (INFINNI) within the framework of Article 28(4) of the GDPR, the Parties expressly agree that:

   a) Any and all references to the "data controller" contained in the SCCs shall be construed as references to the data processor acting as the contracting party that entrusts the processing activities. Such data processor shall assume the obligations and exercise the rights attributed to the "data controller" under the SCCs to the extent that they correspond to it pursuant to the contract entered into with the original data controller and the instructions received therefrom.

   b) Any and all references to the "data processor" contained in the SCCs shall be construed as references to the sub-processor, which shall assume all obligations imposed on the "processor" by the SCCs and shall be bound by the same data protection conditions.

   c) The sub-processor acknowledges and accepts that its activities are carried out within a processing chain in which the original data controller retains ultimate supervisory authority and all rights conferred upon it by the GDPR, including, where applicable, those arising under the third-party beneficiary clause set out in the SCCs.

3. Identification of the applicable scenario. The Parties shall identify in Annex I to the SCCs below whether the specific processing relationship falls under Scenario 1 (Data

Controller – Data Processor) or Scenario 2 (Data Processor – Data Sub-processor), specifying the identity of the original data controller where Scenario 2 applies.

II. Standard Contractual Clauses between controllers and processors under Article 28 (7) of the GDPR

SECTION I
Clause 1
Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses.

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

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

Clause 2
Invariability of the Clauses

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3
Interpretation

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

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

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4
Hierarchy

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

Clause 5 – Optional

Docking clause

(Clause 5 of the SCC is not included and not applicable to this DPA)

SECTION II
OBLIGATIONS OF THE PARTIES

Clause 6
Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7
Obligations of the Parties

7.1. Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

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

7.6. Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

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

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least seven (7) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object. The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

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

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

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

7.8. International transfers

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, INFINNI and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met, as stated in Annex V.

Clause 8
Assistance to the controller

a) The processor shall promptly notify the controller of any requests it has received from the data subject. It shall not respond to the requests itself, unless authorized to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

c) In addition to processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to processor:

    1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

3. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

4. the obligations in Article 32 Regulation (EU) 2016/679.

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9
Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

1. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2. the likely consequences of the personal data breach;

3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III
FINAL PROVISIONS

Clause 10
Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

    1. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

    2. the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;

    3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the processor that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I
List of parties

Customer's Name: _____	Company's Name: INFINNI INNOVATIONS S.A.
Name and role of the Representative: _____ _____	Name and role of the Representative: Mr. Javier Díaz de la Rosa Chief Legal Officer
Date signed: _____	Date signed: 26/10/2026
Corporate Address: _____ _____	Corporate Address: Calle Maria Zambrano 42, Club de Campo Abama Parcela 4-B1 Guia de Isora 38687 Spain

Roles of the Parties

Customer's role: ☐ Controller ☐ Processor	**INFINNI's role**: ☐ Processor ☐ Sub-processor
Identity of the Data Controller: [Please, confirm the identity of the third-party data controller, only applicable when the Customer acts as Processor. Where there are numerous or frequently changing third-party controllers, the Customer may, as soon as reasonably practicable, provide Infinni with a list of the active controllers, which shall be updated at least every 30 days.] _____	
Signature: SIGN HERE	Signature:  SIGN HERE

ANNEX II
Description of the processing

Categories of data subjects whose personal data is processed

The personal data processed concerns the following categories of data subjects:

a) Customers

b) Web Visitors

Categories of personal data processed

The following categories of personal data are processed:

1. Customers

a) Customer's ID, email, avatar, username, earnings, transaction data, vault, PPV, posts, chat history, cookies, logs.

2. Financial Data

a) Payment card details, tax ID, billing address, billing invoice, funds added to wallet, bank account information, pay-out country, pay certificate.

3. Device and technical data

a) Internet or other electronic network activity information, including: Internet Protocol (IP) address (and country code), user agent, device ID, date and time of access, name of your Internet Service Provider, browser type and version, time zone setting, operating system and platform, other technology on the devices you use to access our websites or use our services.

Sensitive data processed (if applicable) and applied restrictions or safeguards

INFINNI may process special categories of personal data as defined under Article 9 GDPR solely to the extent instructed by the Customer and as strictly necessary for the performance of the Services. Appropriate technical and organizational measures are applied to ensure a level of security appropriate to the risk associated with such processing.

Nature of the processing

The nature of the processing operations includes:

a) Collection

b) Storage

c) Analytics

d) Consultation

e) Registration

f) Modification

g) Deletion

a) Extraction

b) Communication by transmission

c) Comparison

d) Use (for security credentials)

e) Translation

Purpose(s) for which the personal data is processed on behalf of the Customer

The personal data is processed for the following purposes:

a) Providing CRM services.

b) Billing, invoicing, and financial operations (including financial center function replacement and payment gateways).

c) Analytics, performance measurement, and service optimization (including growth data analytics).

d) Customer Service Support and resolving technical incidents reported by customers.

e) B2B Client management.

f) Security monitoring, fraud prevention, log retention, and system integrity.

g) Translation services.

h) Transfer of data to third-party services (e.g., Intercom).

i) Application Programming Interface (API).

Duration of the processing

The duration of the Agreement (or as required by applicable law).

ANNEX III
Technical and organizational measures including technical and organizational measures to ensure the security of the data

1. Measures of Pseudonymisation and Encryption of Personal Data

Personal data and customer information are protected through encryption both at rest and in transit.

a) Data stored in databases, file storage and backups are encrypted at rest using the Advanced Encryption Standard with 256-bit keys (AES-256).

b) AWS S3 encryption keys are managed using Amazon S3-managed server-side encryption (SSE-S3), all other keys are centrally managed through Amazon Web Services (AWS) Key Management Service (KMS), with access restricted according to the principle of least privilege.

c) Data transmitted between clients, applications and backend services is protected using HTTPS with Transport Layer Security (TLS) version 1.2 or higher, ensuring confidentiality and integrity of data in transit and preventing man-in-the-middle attacks.

d) Application-Layer Payload Encryption: All API communications between the CRM client and CRM servers use additional advanced encryption algorithms to further protect data payloads beyond standard transport-layer security.

User passwords are never stored in plaintext and are securely stored using strong cryptographic hashing algorithms with appropriate salting mechanisms.

2. Measures for Ensuring Ongoing Confidentiality, Integrity, Availability and Resilience

Technical and organisational measures are implemented to ensure the ongoing confidentiality, integrity, availability and resilience of systems processing personal data.

a) Code Review: All code changes require peer review via Pull Requests (GitHub/GitLab) before being merged.

b) Segregation of Environments: We strictly separate Development, Staging, and Production environments.

c) Multi-Platform Integrity & Signature Verification: We implement robust digital signature verification across all supported platforms to ensure that application binaries are authentic and unmodified. This measure ensures that only authorized code is executed, preventing unauthorized modifications or malicious injections.

d) Application Anti-Tampering Protocols: Our applications utilize active anti-tampering mechanisms that perform runtime integrity checks. These protocols verify the application's signature against the original package, ensuring the environment remains secure and resilient against tampering throughout its lifecycle.

e) Secure Preloading & Resource Integrity: We utilize advanced preloading strategies that incorporate cryptographic integrity validation for critical assets, headers, and configuration files. This ensures that all resources are verified prior to execution, mitigating risks associated with resource interception or manipulation during delivery.

f) Test Data: We do not use real customer personal data in development/testing environments unless strictly anonymized.

3. Measures for Ensuring the Ability to Restore Availability and Access

Measures are implemented to ensure the ability to restore the availability and access to personal data in a timely manner following physical or technical incidents.

a) Automated backups are performed on a daily basis for critical production systems.

b) Backups are retained for 3 to 14 days.

    1. Database backups are retained for 7 days.

    2. OpenSearch backups are retained for 14 days.

    3. Redis backups are retained for 3 days.

c) INFINNI operates with defined recovery objectives, including:

    1. A target Recovery Time Objective (RTO) of up to 24 hours.

    2. A target Recovery Point Objective (RPO) of up to 24 hours, depending on the nature of the incident and the affected systems.

d) Backup data is protected using the same encryption and access control mechanisms applied to production environments.

e) Verification of the integrity of our backups is assured by performing restoration tests quarterly.

4. Processes for Testing, Assessing and Evaluating Security Measures

The effectiveness of technical and organisational measures is reviewed and evaluated on a regular basis.

a) Formal reviews of access controls, logging configurations, and backup and recovery procedures are conducted at least annually, and additionally following significant system changes or security incidents.

b) Security testing activities include external vulnerability scanning of internet-facing systems and external penetration testing performed by qualified third-party security providers annualy.

c) Software Composition Analysis (SCA) is integrated into the GitLab CI/CD pipeline to continuously scan dependencies and the software supply chain for known vulnerabilities.

d) Identified findings are assessed and addressed as part of the organisation’s security and risk management processes.

5. Measures for User Identification and Authorisation

Measures are in place to ensure secure user identification and authorisation.

a) Internal Systems and Infrastructure: Multi-Factor Authentication (MFA) / Two-Factor Authentication (2FA) is strictly enforced for all personnel accessing internal systems, production environments, and administrative interfaces. Authentication is managed via AWS Cognito and Cloudflare to ensure an additional layer of safeguard.

b) Application and Product Access: The CRM application natively supports MFA/2FA capabilities. While available for all users to ensure secure access, enforcement at the application level is currently optional and managed based on user configuration.

c) Access Control: Role-based access controls (RBAC) are implemented across all platforms. These controls ensure that access to personal data is restricted exclusively to authorized personnel whose specific roles require such access, following the principle of least privilege.

d) Zero Trust Architecture: For our critical internal systems, we employ a Zero Trust security approach, enforcing continuous verification of both user identity and device posture to ensure secure access control.

6. Measures for the Protection of Data During Transmission

Personal data transmitted between systems is protected using encrypted communication channels (TLS 1.2 or higher) to ensure confidentiality and integrity during transmission.

7. Measures for the Protection of Data During Storage

Personal data stored in databases, file storage and backups are protected using strong encryption mechanisms (AES-256) managed via AWS KMS.
Access to stored data is restricted and logged.

8. Measures for Ensuring Physical Security

Personal data is processed and stored in cloud infrastructure operated by AWS.
AWS applies industry-standard physical security measures, including controlled access to data centres, surveillance, and environmental protections.
Physical access to data centre facilities is managed exclusively by the cloud service provider.

9. Measures for Ensuring Event Logging

Measures are implemented to ensure logging and traceability of activities related to systems processing personal data.

a) Gateway and application events are logged for security monitoring, troubleshooting and incident investigation. Operational logs are retained for approximately 10 days, while selected security-relevant logs are retained for six (6) months to support audit and traceability requirements.

b) Database audit logging is enabled for core production databases to record data access and modification activities. Audit logs are retained for one (1) month.

Access to logs is restricted to authorised personnel only.

10. Measures for System Configuration and Default Security Settings

Systems are configured using secure default configurations.

a) Security-relevant configurations are maintained and reviewed.

b) Changes to production systems are subject to controlled internal change management processes.

c) Configuration management aims to reduce the risk of misconfiguration and unauthorised changes.

11. Measures for Internal IT and IT Security Governance

Internal governance measures are implemented to ensure the secure management of systems and security.

a) Responsibilities for system administration, access management and security are clearly defined.

b) Access to production systems is restricted and monitored.

c) Mandatory security awareness training is provided to employees handling personal data, including training on data protection and information security principles. Such training is conducted at least annually.

12. Measures for Ensuring Data Minimisation, Data Quality, Retention and Deletion

a) Personal data collected and processed is limited to what is strictly necessary for the provision of services (data minimisation).

b) Reasonable measures are taken to ensure that personal data processed is accurate and up to date (data quality).

c) Personal data is deleted:

    1. Upon termination of the contract, unless retention is required by applicable law.

    2. In response to an explicit request: Deletion is carried out upon a user's explicit request for account closure or data erasure, ensuring the exercise of data subject rights.

d) Logs and backup data are retained only for the specific periods described in Section 9 and are not retained longer than necessary.

13. Measures for Ensuring Accountability and Assistance to the Customer

INFINNI implements appropriate measures to ensure accountability for personal data processing activities.
INFINNI provides assistance to the Customer by redirecting the data subject through a dedicated security and privacy ticketing system.
Privacy-related requests submitted through this channel are acknowledged and redirected to the Customer without undue delay, typically within 48 hours.

ANNEX IV
List of sub-processors

The Customer authorizes the use of the following sub-processors:

1. **Name: AWS**
   - **Address:** Amazon Web Services, Inc. 410 Terry Ave.N., Seattle, WA 98109-5210, United States
   - **Contact:** +1 206-266-4064
   - **Website:** https://aws.amazon.com/
   - **Description of the processing:** Database Storage & Redis & S3 Storage & EBS Storage & CDN & EC2 & Cloud Hosting
   - **Server Location:** European Union

2. **Name: Cloudflare**
   - **Address:** Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107 USA
   - **Contact:** +1 (650) 319-8930
   - **Website:** https://www.cloudflare.com/
   - **Description of the processing:** Provides content delivery network (CDN), DNS, and web security services to ensure secure and performant access
   - **Server Location:** European Union

3. **Name: DeepL**
   - **Address:** Maarweg 165 50825 Cologne Germany
   - **Contact:** +49 221 95018653
   - **Website:** https://www.deepl.com/
   - **Description of the processing:** Translation
   - **Server Location:** European Union

4. **Name: Gemini**
   - **Address:** Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States
   - **Contact:** +1 650-253-0000
   - **Website:** https://gemini.google.com/
   - **Description of the processing:** Translation
   - **Server Location:** European Union

5. **Name: Intercom**
   - **Address:** 55 2nd Street, 4th Floor, San Francisco, CA 94105
   - **Contact:** +1 (888) 222-6056
   - **Website:** https://app.eu.intercom.com/
   - **Description of the processing:** Customer Support ticketing chat
   - **Server Location:** European Union

6. **Name: langsmith**
   - **Address:** LangChain Inc., 501 2nd Street, Suite 120, San Francisco, CA 94107, United States
   - **Contact:** support@langchain.dev
   - **Website:** https://smith.langchain.com/
   - **Description of the processing:** LLM trace observability
   - **Server Location:** European Union

7. **Name: Make.com**

- **Address:** Celonis Inc., One World Trade Center, 87th Floor, New York, NY 10007, USA
- **Contact:** privacy@make.com
- **Website:** https://www.make.com/
- **Description of the processing:** Workflow automation platform
- **Server Location:** European Union

8. **Name: netsuite**
   - **Address:** Oracle Corporation. 2300 Oracle Way Austin, TX 78741 United States
   - **Contact:** +1-877-638-7848
   - **Website:** https://www.netsuite.com/
   - **Description of the processing:** Payment, billing, and invoice management platform.
   - **Server Location:** European Union

9. **Name: OpenRouter**
   - **Address:** OpenRouter, Inc., 169 Madison Avenue, New York, NY 10016, United States
   - **Contact:** support@openrouter.ai
   - **Website:** https://openrouter.ai/
   - **Description of the processing:** LLM model routing / inference API provider
   - **Server Location:** European Union

10. **Name: ovhcloud**
    - **Address:** 11950 Democracy Drive Suite 300 Reston, VA 20190
    - **Contact:** +1-855-684-5463
    - **Website:** https://us.ovhcloud.com/
    - **Description of the processing:** Proxy Machine Provider
    - **Server Location:** European Union

11. **Name: Parasail**
    - **Address:** Parasail, Inc., 4 West 4th Avenue, San Mateo, CA 94402, United States
    - **Contact:** hello@parasail.io
    - **Website:** https://www.saas.parasail.io/
    - **Description of the processing:** LLM inference cloud / GPU infrastructure provider
    - **Server Location:** European Union

12. **Name: Runpod**
    - **Address:** 1181 Nixon Dr. #1158, Moorestown, NJ 08057, United States
    - **Contact:** help@runpod.io
    - **Website:** https://console.runpod.io/
    - **Description of the processing:** LLM inference cloud / GPU infrastructure provider
    - **Server Location:** European Union

13. **Name: Seed**
    - **Address:** BytePlus Pte. Ltd.1 Raffles Quay, #26-10 Singapore
    - **Contact:** contact@byteplus.com
    - **Website:** https://www.byteplus.com/en
    - **Description of the processing:** Translation
    - **Server Location:** European Union

14. **Name: Segment**
    - **Address:** Twilio Segment. 100 California Street, Suite 700, San Francisco, CA 94111, United States

- **Contact:** +1-844-859-7411
- **Website:** https://segment.com/
- **Description of the processing:** Data Forwarding Platform
- **Server Location:** European Union

15. **Name: txtMate**
    - **Address:** Frankfurt, Germany
    - **Contact:** info@txtmate.de
    - **Website:** https://txtmate.de/
    - **Description of the processing:** Translation
    - **Server Location:** European Union

Updates: The current list of sub-processors will be available at any moment in the Legal Center available on our website. INFINNI will update it before engaging any new sub-processor. The Customer may subscribe to notifications of such updates by sending a request to dpo@infinni.io.

APPENDIX I
STANDARD CONTRACTUAL CLAUSES
FOR INTERNATIONAL DATA TRANSFERS

SECTION I

Clause 1
Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

b) The Parties:

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

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

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

c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

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

Clause 2
Effect and invariability of the Clauses

a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3
Third-party beneficiaries

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

    1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

    2. Clause 8 – Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

    3. Clause 9 – Module Three: Clause 9(a), (c), (d) and (e);

    4. Clause 12 – Module Three: Clause 12(a), (d) and (f);

    5. Clause 13;

    6. Clause 15.1(c), (d) and (e);

    7. Clause 16(e);

    8. Clause 18 – Module Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4
Interpretation

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

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

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

Clause 5
Hierarchy

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

Clause 6
Description of the transfer(s)

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

SECTION II
OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

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

b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

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

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

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

8.9 Documentation and compliance

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

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

c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

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

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

MODULE FOUR: Transfer processor to controller

8.1 Instructions

a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "**personal data breach**"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9
Use of sub-processors

MODULE THREE: Transfer processor to processor

a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least seven (7) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

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

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

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

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

Clause 10
Data subject rights

MODULE THREE: Transfer processor to processor

a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the

exercise of their rights under Regulation (EU) 2016/679, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11
Redress

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

MODULE THREE: Transfer processor to processor

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

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

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

2. refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12
Liability

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

MODULE FOUR: Transfer processor to controller

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

b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

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

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

Clause 13
Supervision

MODULE THREE: Transfer processor to processor

a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in the letter c) of this Clause, shall act as competent supervisory authority.

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

c) The competent supervisory authority identified is the Agencia Española de Protección de Datos (AEPD).

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

Clause 14
Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and

agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

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

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

f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [**for Module Three:** , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [**for Module Three:** the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

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

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

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

[**For Module Three:** The data exporter shall forward the notification to the controller.]

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

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

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

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

15.2 Review of legality and data minimisation

a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV
FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

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

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

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

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

2. the data importer is in substantial or persistent breach of these Clauses; or

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

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

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

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

Clause 17
Governing law

MODULE THREE: Transfer processor to processor

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

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Spain.

Clause 18
Choice of forum and jurisdiction

MODULE THREE: Transfer processor to processor

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

b) The Parties agree that those shall be the courts of Santa Cruz de Tenerife – Spain.

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

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

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of Santa Cruz de Tenerife – Spain.

ANNEX I

A. List of parties

Customer's Name: _____	Company's Name: INFINNI INNOVATIONS S.A.
Name and role of the Representative and/or Data Protection Officer: _____ _____	Name and role of the Representative and/or Data Protection Officer: Mr. Javier Díaz de la Rosa Chief Legal Officer
Contact Details: _____	Contact Details: legal@infinni.io
Date signed: _____	Date signed: 26/10/2026
Corporate Address: _____ _____	Corporate Address: Calle Maria Zambrano 42, Club de Campo Abama Parcela 4-B1 Guia de Isora 38687 Spain

Roles of the Parties

Customer's (importer) role: ☐ Controller ☐ Processor	**INFINNI's (exporter) role**: ☐ Processor ☐ Sub-processor
Identity of the Data Controller: [Please, confirm the identity of the third-party data controller, only applicable when the Customer acts as Processor. Where there are numerous or frequently changing third-party controllers carrying out international data transfers, the Customer may, as soon as reasonably practicable, provide Infinni with a list of the active controllers, which shall be updated at least every 30 days] _____	
Signature: SIGN HERE	Signature:  SIGN HERE

B. Description of the processing

Categories of data subjects whose personal data is transferred

The personal data processed concerns the following categories of data subjects:

a) Customers

b) Web Visitors

Categories of personal data transferred

The following categories of personal data are processed:

1. Customers

a) Customer's ID, email, avatar, username, earnings, transaction data, vault, PPV, posts, chat history, cookies, logs.

2. Financial Data

a) Payment card details, tax ID, billing address, billing invoice, funds added to wallet, bank account information, pay-out country, pay certificate.

3. Device and technical data

a) Internet or other electronic network activity information, including: Internet Protocol (IP) address (and country code), user agent, device ID, date and time of access, name of your Internet Service Provider, browser type and version, time zone setting, operating system and platform, other technology on the devices you use to access our websites or use our services.

Sensitive data processed (if applicable) and applied restrictions or safeguards

INFINNI may process special categories of personal data as defined under Article 9 GDPR solely to the extent instructed by the Customer and as strictly necessary for the performance of the Services. Appropriate technical and organizational measures are applied to ensure a level of security appropriate to the risk associated with such processing.

Nature of the processing

The nature of the processing operations includes:

a) Collection

b) Storage

c) Analytics

d) Consultation

e) Registration

f) Modification

g) Deletion

h) Extraction

i) Communication by transmission

j) Comparison

k) Use (for security credentials)

l) Translation

Purpose(s) for which the personal data is transfer and further processing

The personal data is processed for the following purposes:

a) Providing CRM services.

b) Billing, invoicing, and financial operations (including financial center function replacement and payment gateways).

c) Analytics, performance measurement, and service optimization (including growth data analytics).

d) Customer Service Support and resolving technical incidents reported by customers.

e) B2B Client management.

f) Security monitoring, fraud prevention, log retention, and system integrity.

g) Translation services.

h) Transfer of data to third-party services (e.g., Intercom).

i) Application Programming Interface (API).

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

_____

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

_____

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

_____

ANNEX II

Technical and organizational measures including technical and organizational measures to ensure the security of the data

MODULE THREE: Transfer processor to processor

1. Measures of Pseudonymisation and Encryption of Personal Data

Personal data and customer information are protected through encryption both at rest and in transit.

a) Data stored in databases, file storage and backups are encrypted at rest using the Advanced Encryption Standard with 256-bit keys (AES-256).

b) AWS S3 encryption keys are managed using Amazon S3-managed server-side encryption (SSE-S3), all other keys are centrally managed through Amazon Web Services (AWS) Key Management Service (KMS), with access restricted according to the principle of least privilege.

c) Data transmitted between clients, applications and backend services is protected using HTTPS with Transport Layer Security (TLS) version 1.2 or higher, ensuring confidentiality and integrity of data in transit and preventing man-in-the-middle attacks.

d) Application-Layer Payload Encryption: All API communications between the CRM client and CRM servers use additional advanced encryption algorithms to further protect data payloads beyond standard transport-layer security.

User passwords are never stored in plaintext and are securely stored using strong cryptographic hashing algorithms with appropriate salting mechanisms.

2. Measures for Ensuring Ongoing Confidentiality, Integrity, Availability and Resilience

Technical and organisational measures are implemented to ensure the ongoing confidentiality, integrity, availability and resilience of systems processing personal data.

a) Code Review: All code changes require peer review via Pull Requests (GitHub/GitLab) before being merged.

b) Segregation of Environments: We strictly separate Development, Staging, and Production environments.

c) Multi-Platform Integrity & Signature Verification: We implement robust digital signature verification across all supported platforms to ensure that application binaries are authentic and unmodified. This measure ensures that only authorized code is executed, preventing unauthorized modifications or malicious injections.

d) Application Anti-Tampering Protocols: Our applications utilize active anti-tampering mechanisms that perform runtime integrity checks. These protocols verify the application's signature against the original package, ensuring the environment remains secure and resilient against tampering throughout its lifecycle.

e) Secure Preloading & Resource Integrity: We utilize advanced preloading strategies that incorporate cryptographic integrity validation for critical assets, headers, and

configuration files. This ensures that all resources are verified prior to execution, mitigating risks associated with resource interception or manipulation during delivery.

f) Test Data: We do not use real customer personal data in development/testing environments unless strictly anonymized.

3. Measures for Ensuring the Ability to Restore Availability and Access

Measures are implemented to ensure the ability to restore the availability and access to personal data in a timely manner following physical or technical incidents.

a) Automated backups are performed on a daily basis for critical production systems.

b) Backups are retained for 3 to 14 days.

    1. Database backups are retained for 7 days.

    2. OpenSearch backups are retained for 14 days.

    3. Redis backups are retained for 3 days.

c) INFINNI operates with defined recovery objectives, including:

    1. A target Recovery Time Objective (RTO) of up to 24 hours.

    2. A target Recovery Point Objective (RPO) of up to 24 hours, depending on the nature of the incident and the affected systems.

d) Backup data is protected using the same encryption and access control mechanisms applied to production environments.

e) Verification of the integrity of our backups is assured by performing restoration tests quarterly.

4. Processes for Testing, Assessing and Evaluating Security Measures

The effectiveness of technical and organisational measures is reviewed and evaluated on a regular basis.

a) Formal reviews of access controls, logging configurations, and backup and recovery procedures are conducted at least annually, and additionally following significant system changes or security incidents.

b) Security testing activities include external vulnerability scanning of internet-facing systems and external penetration testing performed by qualified third-party security providers annualy.

c) Software Composition Analysis (SCA) is integrated into the GitLab CI/CD pipeline to continuously scan dependencies and the software supply chain for known vulnerabilities.

d) Identified findings are assessed and addressed as part of the organisation’s security and risk management processes.

5. Measures for User Identification and Authorisation

Measures are in place to ensure secure user identification and authorisation.

a) Internal Systems and Infrastructure: Multi-Factor Authentication (MFA) / Two-Factor Authentication (2FA) is strictly enforced for all personnel accessing internal systems, production environments, and administrative interfaces. Authentication is managed via AWS Cognito and Cloudflare to ensure an additional layer of safeguard.

b) Application and Product Access: The CRM application natively supports MFA/2FA capabilities. While available for all users to ensure secure access, enforcement at the application level is currently optional and managed based on user configuration.

c) Access Control: Role-based access controls (RBAC) are implemented across all platforms. These controls ensure that access to personal data is restricted exclusively to authorized personnel whose specific roles require such access, following the principle of least privilege.

d) Zero Trust Architecture: For our critical internal systems, we employ a Zero Trust security approach, enforcing continuous verification of both user identity and device posture to ensure secure access control.

6. Measures for the Protection of Data During Transmission

Personal data transmitted between systems is protected using encrypted communication channels (TLS 1.2 or higher) to ensure confidentiality and integrity during transmission.

7. Measures for the Protection of Data During Storage

Personal data stored in databases, file storage and backups are protected using strong encryption mechanisms (AES-256) managed via AWS KMS.
Access to stored data is restricted and logged.

8. Measures for Ensuring Physical Security

Personal data is processed and stored in cloud infrastructure operated by AWS.
AWS applies industry-standard physical security measures, including controlled access to data centres, surveillance, and environmental protections.
Physical access to data centre facilities is managed exclusively by the cloud service provider.

9. Measures for Ensuring Event Logging

Measures are implemented to ensure logging and traceability of activities related to systems processing personal data.

a) Gateway and application events are logged for security monitoring, troubleshooting and incident investigation. Operational logs are retained for approximately 10 days, while selected security-relevant logs are retained for six (6) months to support audit and traceability requirements.

b) Database audit logging is enabled for core production databases to record data access and modification activities. Audit logs are retained for one (1) month.

Access to logs is restricted to authorised personnel only.

10. Measures for System Configuration and Default Security Settings

Systems are configured using secure default configurations.

a) Security-relevant configurations are maintained and reviewed.

b) Changes to production systems are subject to controlled internal change management processes.

c) Configuration management aims to reduce the risk of misconfiguration and unauthorised changes.

11. Measures for Internal IT and IT Security Governance

Internal governance measures are implemented to ensure the secure management of systems and security.

a) Responsibilities for system administration, access management and security are clearly defined.

b) Access to production systems is restricted and monitored.

c) Mandatory security awareness training is provided to employees handling personal data, including training on data protection and information security principles. Such training is conducted at least annually.

12. Measures for Ensuring Data Minimisation, Data Quality, Retention and Deletion

a) Personal data collected and processed is limited to what is strictly necessary for the provision of services (data minimisation).

b) Reasonable measures are taken to ensure that personal data processed is accurate and up to date (data quality).

c) Personal data is deleted:

    3. Upon termination of the contract, unless retention is required by applicable law.

    4. In response to an explicit request: Deletion is carried out upon a user's explicit request for account closure or data erasure, ensuring the exercise of data subject rights.

d) Logs and backup data are retained only for the specific periods described in Section 9 and are not retained longer than necessary.

13. Measures for Ensuring Accountability and Assistance to the Customer

INFINNI implements appropriate measures to ensure accountability for personal data processing activities.
INFINNI provides assistance to the Customer by redirecting the data subject through a dedicated security and privacy ticketing system.
Privacy-related requests submitted through this channel are acknowledged and redirected to the Customer without undue delay, typically within 48 hours.