Ver. 1.1 (January 2026)

Data Processing Addendum

Acsense Inc. ("**Recipient**") and the customer ("**Customer**"; each a "**Party**", together the "**Parties**"), have entered into a principal agreement ("**Agreement**") in the context of which Personal Data (as defined below) is disclosed to or processed by the Recipient, and are agreeing to this Data Protection Addendum, including Schedule A and Annexes I-III ("**DPA**"). This DPA is entered into by Customer and Recipient and supplements the Agreement.

1. **Introduction**

1.1 This DPA reflects the Parties' agreement on the processing of Personal Data in connection with the Data Protection Laws.

1.2 Any ambiguity in this DPA shall be resolved to permit the Parties to comply with all Data Protection Laws.

1.3 In the event and to the extent that the Data Protection Laws impose stricter obligations on the Parties than under this DPA, the Data Protection Laws shall prevail.

2. **Definitions and Interpretation**

2.1 In this DPA:

2.1.1 "**Approved Jurisdiction**" means a jurisdiction approved as having adequate legal protections for data by the European Commission, the UK Information Commissioner's Office, or the Federal Data Protection and Information Commissioner (FDPIC) where applicable.

2.1.2 "**Data Protection Laws**" means, any and all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or federal or national level, pertaining to data privacy, data security or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"), the Data Protection Act 2018 and the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the Swiss Federal Act on Data Protection ("**FADP**"), the US Data Protection Laws, and any amendments or replacements to the foregoing.

2.1.3 "**Data Subject**" means a natural person to whom Personal Data relates. Where applicable, the term Data Subject shall include "**Consumer**", as this term is defined under US Data Protection Laws.

2.1.4 "**Security Incident**" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. For the avoidance of doubt, any Security Incident shall be regarded as a personal data breach as defined in the GDPR, a breach of data security as defined in the FADP or as otherwise defined under Data Protection Laws.

2.1.5 "**Special Categories of Data**" means personal data as defined under Article 9 of the GDPR and where applicable, sensitive personal data as defined under the FADP or sensitive personal information, as defined under US Data Protection Laws.

2.1.6 "**Standard Contractual Clauses**" means the applicable module of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council from June 4th 2021, as available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.

2.1.7 "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, which was entered into force on 21 March, 2022.

2.1.8 "**US Data Protection Laws**" means, any and all applicable laws, rules, acts, decrees, directives, regulations and binding regulatory guidance, on any state or federal level, pertaining to data privacy, data security and the protection of Personal Data, including, without limitation, in California, Colorado, Connecticut, Utah, Virginia, Texas, Oregon, Florida, Montana, Iowa, Delaware, New Jersey, New Hampshire, Nebraska, as well as any future laws, amendments, or regulations that may be enacted or promulgated governing data protection within the United States.

2.1.9 The terms "**controller**", "**Personal Data**" "**process(ing)**" and "**processor**" as used in this DPA have the meanings given to them in Data Protection Laws. Where applicable, controller shall be deemed "**Business**", processor shall be deemed "**Service Provider**" or "**Contractor**", and Personal Data shall be deemed "**Personal Information**" as these terms are defined under US Data Protection Laws.

2.1.10 Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

3. **Application of this DPA**

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

3.1.1 Recipient processes Personal Data that is made available by the Customer in connection with the Agreement;

3.1.2 Any of the Data Protection Laws apply to the processing of Personal Data.

4. **Roles and Restrictions on Processing**

4.1 The Parties acknowledge that Customer is either: (a) a controller of Personal Data; or (b) acting as a Processor on behalf of other controllers and has been instructed and authorized by such controllers to the processing of Personal Data by Recipient as Customer's subprocessor, as set forth in this DPA.

4.2 If Recipient has access to or otherwise processes Personal Data pursuant to the Agreement, then Recipient shall:

4.2.1 only process the Personal Data in accordance with Customer's documented instructions and on its behalf, and in accordance with the Agreement and this DPA and related Attachments, unless required otherwise under applicable laws. In such case, Recipient shall, to the extent legally permitted, promptly notify Customer of such legal obligation. The duration, nature and purposes of the processing, as well as the types of Personal Data processed and categories of Data Subjects processed under this DPA are further specified in Annex I of this DPA;

4.2.2 take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and process Personal Data; ensure persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and ensure that such personnel are aware of their responsibilities under this DPA and any Data Protection Laws;

4.2.3 promptly, and in any case within the period of time required in Data Protection Laws, assist Customer as needed to cooperate with and respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information (including details of the services provided by Recipient) related to Recipient's processing of Personal Data;

4.2.4 notify the Customer without undue delay, and no later than twenty four (24) hours, after becoming aware of a Security Incident;

4.2.5 upon receipt of: (a) requests from Data Subjects to exercise their rights, as applicable, under the Data Protection Laws in connection with Personal Data processed under this DPA; or (b) any requests or inquiries from supervisory authorities, customers, or others, to provide information related to Recipient's processing of Personal Data under this DPA; the Recipient shall: (i) direct such requests to Customer without undue delay, (ii) not respond or act upon such requests without prior written approval from Customer; and (iii) promptly, and in any case within the period of time required in Data Protection Laws, provide full, reasonable cooperation and assistance to Customer in responding to and exercising such requests;

4.2.5.1 ensure compliance with its obligation, or the obligation of its customers, to carry out data protection impact assessments with respect to the processing of Personal Data, and with the obligation of prior consultation with the supervisory authority obligation (if applicable);

4.2.6 only process or use Personal Data on its systems or facilities to the extent necessary to perform its obligations under the Agreement or this DPA;

4.2.7 maintain accurate written records of any and all the processing activities of any Personal Data carried out under the Agreement (including the categories of processing carried out and opt-out requests submitted, if applicable), and shall make such records available to the Customer and applicable supervisory authority on request;

4.2.8 to the extent feasible, make all reasonable efforts to ensure that Personal Data are accurate and up to date at all times while in its custody or under its control;

4.2.9 Save for as explicitly permitted hereunder, not disclose, lease, sell, share, make available, disseminate, or otherwise distribute Personal Data;

4.2.10 promptly notify Customer of any investigation, litigation, arbitrated matter or other dispute relating to the Recipient or the processing of Personal Data under the Agreement;

4.2.11 promptly notify Customer in writing and provide Customer an opportunity to intervene in any judicial, enforcement, or administrative process if Recipient is required to disclose any Personal Data to any person other than Customer (unless Recipient legally prohibited from doing so);

4.2.12 upon termination of the Agreement, or upon Customer's written request at any time during the term of the Agreement, Recipient shall cease to process any Personal Data received from Customer, and within thirty (30) days will at the request of Customer: (1) return the Personal Data; or (2) securely and completely destroy or erase all Personal Data in its possession or control (including any copies thereof), unless and solely to the extent the foregoing conflicts with any applicable laws. In such case, Recipient shall notify the Customer and only process such Personal Data in order to comply with its legal obligations. The terms of this DPA shall remain applicable to the processing of such Personal Data until returned or erased. At Customer's request, Recipient shall give Customer a certificate confirming that it has fully complied with the requirements of this clause.

5. **Sub-processing**

5.1 Customer provides a general authorization to Company to appoint (and permit each Sub-Processor appointed in accordance with this section to appoint) Processors and/or Sub Processors in accordance with this section.

5.2 Company may continue to use those Processors and/or Sub Processors already engaged by Company as at the date of this Agreement, subject to Company in each case as soon as practicable meeting the obligations set out in this section. A list of the Company's current Sub Processors is attached as Annex III.

5.3 Company can at any time and without justification appoint a new Processor and/or Sub-Processor provided that Company provides fifteen (15) days' prior written notice and the Customer does not legitimately object to such changes within that timeframe.. To the extent Customer objects to the appointment of any new Sub-processor, the Parties shall negotiate in good faith this objection. In the event the Parties, acting reasonably and in good faith, have not reached an amicable solution, then Customer may terminate the portion of the Agreement that requires the employment of said Sub-processor.

5.4 Recipient will execute a written agreement with such approved Sub-processor containing terms providing at least equivalent protection of Personal Data as provided under this DPA.

5.5 Recipient shall have a written security policy that provides guidance to its Sub-processors to ensure the security, confidentiality, integrity and availability of Personal Data and systems maintained or processed by Recipient.

5.6 Customer may require Recipient to provide Customer with full details of the proposed Sub-processor's involvement including but not limited to the identity of the Sub-processor, its data security record, the location of its processing facilities and a description of the access to Personal Data proposed.

5.7 Recipient shall be fully liable for the acts or omissions of Sub-processors to the same extent it is liable for its own actions or omissions under this DPA and Data Protection Laws.

6. **Transfer of Personal Data**

6.1 Where the GDPR, UK GDPR, or FADP are applicable, to the extent Recipient processes Personal Data outside the EEA, the UK, Switzerland (respectively), or an Approved Jurisdiction, the parties shall enter into the Standard Contractual Clauses and UK Addendum (as applicable) subject to any amendments contained in Schedule A, in which event: (i) the Standard Contractual Clauses and the UK Addendum are incorporated herein by reference; and (ii) Customer shall be deemed data exporter and the Recipient shall be deemed data importer (as these terms are defined therein).

6.2 Where the GDPR, UK GDPR or FADP are applicable, to the extent Recipient's Sub-processor processes Personal Data outside the EEA, the UK, Switzerland (respectively), or an Approved Jurisdiction, such transfer shall be based on one of the appropriate safeguards specified in the GDPR, UK GDPR, or FADP (as applicable).

6.3 If Recipient and/or its Sub-processors intend to rely on Standard Contractual Clauses and, where applicable the UK Addendum, then if the Standard Contractual Clauses or the UK Addendum are superseded by new or modified mechanism, the new or modified mechanism shall be deemed to be incorporated into this DPA, and Recipient will

promptly begin complying with such mechanism. Recipient will abide by the obligations set forth under the Standard Contractual Clauses and UK Addendum.

7. **Security Standards**

7.1 Recipient shall implement and maintain commercially reasonable and appropriate physical, technical and organizational security measures to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access to Personal Data transmitted, stored or otherwise processed; and all other unlawful forms of processing; as detailed in Annex II.

7.2 To the extent that Recipient processes Special Categories of Data, the security measures referred to in this DPA shall also include, at a minimum (i) routine risk assessments of Recipient's information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while "at rest" and during transmission (whether sent by e-mail, fax, or otherwise), and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone).

8. **Obligations under US Data Protection Laws**

8.1 To the extent that Recipient processes Personal Data which is subject to US Data Protection Laws, then in addition to the obligations set out herein, Recipient shall not:

8.1.1 process the Personal Data other than on Customer's documented instructions;

8.1.2 sell or share Personal Data (as the terms "sell" and "share" are defined under US Data Protection Laws) disclosed to or collected by it (or on its behalf) in connection with the Agreement, or, except as necessary to perform the Services, retain, collect, use or disclose said Personal Data, for any purpose, including commercial purposes, other than for the business purpose (as defined under US Data Protection Laws);

8.1.3 retain, use or disclose the personal information disclosed to it or collected by it (or on its behalf) in connection with the Agreement, outside the direct business relationship between the Customer and the Recipient, unless otherwise permitted under US Data Protection Laws;

8.1.4 combine the Personal Data of consumers that it collects, receives from, or on behalf of, the Customer with Personal Data that the Recipient receives from, or on behalf of, another person or persons or collects from its own interaction with consumers unless and solely to the extent necessary to perform the business purpose.

8.2 Recipient acknowledges and understands its obligations under this clause, and will comply with them.

9. **General**

9.1 If this DPA does not specifically address a particular data security or privacy standard or obligation, Recipient will use appropriate, generally accepted practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of Personal Data.

9.2 If Recipient is unable to provide the level of protection as required herein or to abide to its obligations under this DPA or Data Protection Laws, Recipient shall immediately notify Customer and cease processing. Any non-compliance with the requirements herein shall be deemed a material breach of the Agreement and Customer shall have the right to terminate the Agreement immediately without penalty.

9.3 Customer shall have the right to require Recipient (a) to promptly provide it with all information necessary to, and (b) conduct its own audits and inspections of Recipient (including its facilities or equipment involved in the processing of Personal Data) in order to: demonstrate compliance with the DPA and Data Protection Laws. The Recipient shall allow and contribute to such audits and inspections. Where possible, audits and inspections shall be conducted with reasonable advanced notice to Recipient, and shall take place during normal business hours to reasonably limit any disruption to Recipient's business.

9.4 Recipient will indemnify Customer and hold Customer harmless from any cost, charge, damages, expenses or losses incurred as a result of Recipient's breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon Customer promptly notifying Recipient of a claim, and providing reasonable cooperation and assistance to Recipient in defense of such claim.

10. **Priority**

10.1 If there is any conflict or inconsistency between the terms of this DPA and the remainder of the Agreement then, the terms of this DPA will govern. Subject to the amendments in this DPA, the Agreement remains in full force and effect.

10.2 Unless stated otherwise in the DPA, Standard Contractual Clauses or the UK Addendum, in case of a conflict between the provisions of the DPA and to the provisions of the Standard Contractual Clauses and the UK Addendum, the provisions providing the more stringent protection to Personal Data and the rights of individuals shall govern.

11. **Changes to this DPA**

11.1 The Recipient may amend this DPA from time to time, provided that it gives the other Party prior written notice of such amendment. Any such amendment shall become effective as specified in the notice, unless the other Party objects in writing within the notice period.

11.2 If any of the Data Protection Laws are superseded by new or modified Data Protection Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto, and including changes to the Standard Contractual Clauses or the UK Addendum), the new or modified Data Protection Laws shall be deemed to be incorporated into this DPA, and each Party will promptly begin complying with such Data Protection Laws in respect of its respective processing activities.

Schedule A – Standard Contractual Clauses and the UK Addendum

1. If Customer is a controller – the Parties shall be deemed to enter into the Controller to Processor Standard Contractual Clauses (Module 2); if Customer is a processor – the Parties shall be deemed to enter into the Processor to Processor Standard Contractual Clauses (Module 3).

2. This Schedule A sets out the Parties' agreed interpretation of their respective obligations under Module Two or Module Three of the Standard Contractual Clauses (as applicable).

3. The Parties agree that for the purpose of transfer of Personal Data between the Customer (Data Exporter) and the Recipient (Data Importer), the following shall apply:

   3.1. Clause 7 of the Standard Contractual Clauses shall not be applicable.

   3.2. In Clause 9, Option 1 shall apply. The Data Importer shall submit the request for specific authorization at least thirty (30) days prior to the engagement of the Sub-processor. Annex III shall be updated accordingly.

   3.3. In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.

   3.4. In Clause 17, Option 1 shall apply. The Parties agree that the clauses shall be governed by the law of Ireland.

   3.5. In Clause 18(b) the Parties choose the courts of Dublin as their choice of forum and jurisdiction.

4. Annexes I-III below shall be incorporated into the Standard Contractual Clauses.

5. To the extent the UK Addendum applies, the following shall apply:

   5.1. All the information provided under the Standard Contractual Clauses shall apply to the UK Addendum with the necessary changes per the requirement of the UK Addendum. Annexes 1A, 1B and 2 to the UK Addendum shall be replaced with Annexes I–III below, respectively.

   5.2. In Table 4 of the UK Addendum, either party may terminate the agreement in accordance with section 19 of the UK Addendum.

   5.3. By entering into this Data Protection Agreement, the Parties hereby agree to the format changes made to the UK Addendum.

6. To the extent the FADP applies, the following shall apply:

   6.1. references to the GDPR are to be understood as references to the FADP;

   6.2. the competent supervisory authority shall be the FDPIC;

   6.3. references to 'EU', 'Union' and 'Member State' are replaced with 'Switzerland';

   6.4. In Clause 17, Option 1 shall apply. The Parties agree that the clauses shall be governed by the law of Switzerland;

   6.5. In Clause 18(b) the Parties choose the courts of Zurich Switzerland as their choice of forum and jurisdiction.

Annex I – Description of Processing Activities

A. Identification of Parties

"**Data Exporter**": Customer;

"**Data Importer**": Recipient.

B. Description of Transfer

Categories of data subject:	X Customer's end-users ☐ Customer's employees ☐ Customer's customers ☐ Other: _____
Categories of Personal Data	X Contact information (name, address, telephone number, email address etc.) ☐ Financial and payment data (e.g. credit card number, bank account, transactions) ☐ Governmental IDs (passport, driver's license) x Device identifiers and internet or electronic network activity (IP addresses, GAID/IDFA, browsing history, timestamps) x Geo-location information ☐ Other: _____
Special Categories of Data/Sensitive Personal Information	X None ☐ Genetic or biometric data ☐ Health data ☐ Racial or ethnic origin, religious or philosophical beliefs ☐ Political opinions, religious or philosophical beliefs ☐ Precise Geo-location information ☐ Government identifier (social security, driver's license, state identification card, or passport number) ☐ Financial account and login information ☐ Sexual orientation; ☐ Citizenship or citizenship status; ☐ Known child ☐ Other: _____
Nature of Processing	☐ Storage ☐ Analytics ☐ Advertising (including auditing related to Advertising) ☐ Payment processing ☐ Consultation X Security, integrity and maintaining quality of the Customer's services ☐ Transient use

	☐ Other (including the provision of services of behalf of the Customer): _____
Frequency of Transfer	☐ One-off X Continuous ☐ N/A ☐ Other: _____
Purpose of the transfer and further processing	Providing the Services to Customer.
Retention period	Personal Data will be retained for the term of the Agreement.

Annex II – Technical and Organizational Measures to Ensure the Security of the Data

Description of the technical and organizational measures implemented by the data importer (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Security Management
Recipient maintains a written information security management system (ISMS), in accordance with this Annex, that includes policies, processes, enforcement and controls governing all storage/processing/transmitting of Personal Data, designed to (a) secure Personal Data against accidental or unlawful loss, access or disclosure; (b) identify reasonable foreseeable and internal risks to security and authorized access to Recipient Network, and (c) minimize security risks, including through risk assessment and regular testing. The information security program will include the following measures:

- Recipient actively follows information security trends and developments as well as legal developments with regards to the services provided and especially with regards to Personal Data and uses such insights to maintain its ISMS, as appropriate.
- To the extent Recipient process cardholder or payment data (such as payment or credit cards), Recipient will maintain its ISMS in accordance with the PCI DSS standard, augmented to cover Personal Data, or such other alternative standards that are substantially equivalent to PCI DSS for the establishment, implementation, and control of its ISMS. Additionally, Recipient will be assessed against PCI DSS annually by an on-site assessment carried out by an independent QSA (Qualified Security Assessor) and upon Customer's request, not to exceed once annually, Recipient will provide Customer with PCI DSS attestation of compliance.

Maintain an Information Security Policy
Recipient's ISMS is based on its security policies that are regularly reviewed (at least yearly) and maintained and disseminated to all relevant Parties, including all personnel. Security policies and derived procedures clearly define information security responsibilities including responsibilities for:

- Maintaining security policies and procedures;
- Secure development, operation and maintenance of software and systems;
- Security alert handling;
- Security incident response and escalation procedures;
- User account administration;
- Monitoring and control of all systems as well as access to Personal Data.

Personnel is screened prior to hire and trained (and tested) through a formal security awareness program upon hire and annually. For service providers with whom Personal Data is shared or that could affect the security of Personal Data a process has been set up that includes initial due diligence prior to engagement and regular (typically yearly) monitoring. Personal Data has implemented a risk-assessment process that is based on ISO 27005.

Secure Networks and Systems
Recipient has installed and maintains a firewall configurations to protect Personal Data that controls all traffic allowed between Recipient's (internal) network and untrusted (external) networks, as well as traffic into and out of more sensitive areas within its internal network. This includes current documentation, change control and regular reviews.
Recipient does not use vendor-supplied defaults for system passwords and other security parameters on any systems and has developed configuration standards for all system components consistent with industry-accepted system hardening standards.

Protection of Personal Data
Recipient keeps Personal Data storage to a minimum and implements data retention and disposal policies to limit data storage to that which is necessary, in accordance with the needs of its customers.
Recipient uses strong encryption and hashing for Personal Data anywhere it is stored. Recipient has documented and implemented all necessary procedures to protect (cryptographic) keys used to secure stored Personal Data against disclosure and misuse. All transmission of Personal Data across open, public networks is encrypted using strong cryptography and security protocols.

Vulnerability Management Program
Recipient protects all systems against malware and regularly updates anti-virus software or programs to protect against malware – including viruses, worms, and Trojans. Anti-virus software is used on all systems commonly affected by malware to protect such systems from current and evolving malicious software threats.
Recipient develops and maintains secure systems and applications by:

- Having established and evolving a process to identify and fix (e.g. through patching) security vulnerabilities, that ensures that all systems components and software are protected from known vulnerabilities,
- Developing internal and external software applications, including web-applications, securely using a secure software development process based on best practices, e.g. such as code reviews and OWASP secure coding practices, that incorporates information security throughout the software-development lifecycle,
- Implementing a stringent change management process and procedures for all changes to system components that include strict separation of development and test environments from production environments and prevents the use of production data for testing or development.

Implementation of Strong Access Control Measures

"**Recipient Network**" means the Recipient's data center facilities, servers, networking equipment, and host software systems (e.g. virtual firewalls) as employed by the Recipient to process or store Personal Data.
The Recipient Network will be accessible to employees, contractors and any other person as necessary to provide the services to the Customer. Recipient will maintain access controls and policies to manage what access is allowed to the Recipient Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Recipient will maintain corrective action and incident response plans to respond to potential security threats.
Recipient strictly restricts access to Personal Data on a need to know basis to ensure that critical data can only be accessed by authorized personnel. This is achieved by:

- Limiting access to system components and Personal Data to only those individuals whose job requires such access; and
- Establishing and maintaining an access control system for system components that restricts access based on a user's need to know, with a default "deny-all" setting.

Recipient identifies and authenticates access to all systems components by assigning a unique identification to each person with access. This ensures that each individual is uniquely accountable for its actions and any actions taken on critical data and systems can be traced to known and authorized users and processes. Necessary processes to ensure proper user identification management, including control of addition/deletion/modification/revocation/disabling of IDs and/or credentials as well as lock out of users after repeated failed access attempts and timely termination of idling session, have been implemented.

User authentication utilizes at least passwords that have to meet complexity rules, which need to be changed on a regular basis and which are cryptographically secured during transmission and storage on all system components. All individual non-console and administrative access and all remote access use multi-factor authentication.
Authentication policies and procedures are communicated to all users and group, shared or generic IDs/passwords are strictly prohibited.

Restriction of Physical Access to Personal Data
Any physical access to data or systems that house Personal Data are appropriately restricted using appropriate entry controls and procedures to distinguish between onsite personnel and visitors. Access to sensitive areas is controlled and includes processes for authorization based on job function and access revocation for personnel and visitors.
Media and backups are secured and (internal and external) distribution is strictly controlled. Media containing Personal Data no longer needed for business or legal reasons is rendered unrecoverable or physically destroyed.

Regular Monitoring and Testing of Networks
All access to network resources and Personal Data is tracked and monitored using centralized logging mechanisms that allow thorough tracking, alerting, and analysis on a regular basis (at least daily) as well as when something does go

wrong. All systems are provided with correct and consistent time and audit trails are secured and protected, including file-integrity monitoring to prevent change of existing log data and/or generate alerts in cases of unauthorized access or anomalies of access. Audit trails for critical systems are kept for a year.

Security of systems and processes is regularly tested, at least yearly. This is to ensure that security controls for system components, processes and custom software continue to reflect a changing environment. Security testing includes:

- Processes to test rogue wireless access points;
- Internal and external network vulnerability tests that are carried out at least quarterly. An external, qualified party carries out the external network vulnerability tests;
- External and internal penetration tests using Recipient's penetration test methodology that is based on industry-accepted penetration testing approaches that cover all the relevant systems and include application-layer as well as network-layer tests

All test results are kept on record and any findings are remediated in a timely manner.
Recipient does not allow penetration tests carried out by or on behalf of its customers.
In daily operations IDS (intrusion detection system) is used to detect and alert on intrusions into the network and file-integrity monitoring has been deployed to alert personnel to unauthorized modification of critical systems.

Incident Management
Recipient has implemented and maintains an incident response plan and is prepared to respond immediately to a system breach. Incident management includes:

- Definition of roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of customers,
- Specific incident response procedures,
- Analysis of legal requirements for reporting compromises,
- Coverage of all critical system components,
- Regular review and testing of the plan,
- Incident management personnel that is available 24/7,
- Training of staff,
- Inclusion of alerts from all security monitoring systems,
- Modification and evolution of the plan according to lessons learned and to incorporate industry developments.

Recipient has also implemented a business continuity process (BCP) and a disaster recovery process (DRP) that are maintained and regularly tested. Data backup processes have been implemented and are tested regularly.

Physical Security
Physical Access Controls
Physical components of the Recipient Network are housed in nondescript facilities ("Facilities"). Physical barrier controls are used to prevent unauthorized entrance to Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

Limited Employee and Contractor Access
Recipient provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of Recipient or its affiliates.

Physical Security Protections
All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Recipient also

maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, etc.) with door contacts, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

Continued Evaluation

Recipient will conduct periodic reviews of the Security of its Recipient Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. Recipient will continually evaluate the security of its Recipient Network to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Annex III – List of Sub-processors

Below is the list of the Data Importer's Sub-processors:

1	**Okta**	Address:	100 First Street, 6th Floor San Francisco, CA 94105, USA
		Contact details:	Support: 1-800-219-0964 Other: 1-888-722-7871
		Service Location:	USA
		Description of processing:	Okta is a cloud-based IAM platform that provides identity and access management solutions for workforce and customer applications. Okta enables secure and seamless authentication & authorization.
2	**AWS**	Address:	410 Terry Avenue North, Seattle, Washington, 98109, USA
		Contact details:	+1 (206) 2664064
		Service Location:	USA
		Description of processing:	AWS- Amazon Web Services, a cloud computing platform that for computing infrastructure: EC2, S3, Lambda, RDS etc.,
3	**Cloudflare**	Address:	101 Townsend St., San Francisco, California 94107, USA
		Contact details:	+ 1 888 9935273
		Service Location:	USA
		Description of processing:	Cloudflare is a company that provides content delivery network services, cloud cybersecurity, DDoS mitigation, and ICANN-accredited domain registration services.
4	**HubSpot**	Address:	25 First Street, Cambridge, Massachusetts, 02141, USA
		Contact details:	+1 888 4827768
		Service Location:	USA
		Description of processing:	HubSpot is a SaaS CRM product for inbound marketing, sales, and customer service.
5	**New Relic**	Address:	188 Spear Street, Suite 1200, San Francisco, CA 94105, USA
		Contact details:	+1 (888) 643-8776 +1 (650) 777-7600
		Service Location:	USA
		Description of processing:	New Relic is a cloud-based software platform primarily used for full-stack observability and application performance monitoring (APM)

6	**Trend Micro Vision One**	Address:	US Headquarters Trend Micro Incorporated 225 East John Carpenter Freeway, Suite 1500 Irving, Texas 75062
		Contact details:	+1 (817) 569-8900 Toll-free: (888) 762-8736
		Service Location:	USA
		Description of processing:	cybersecurity platform for extended detection and response (XDR) capabilities. It provides a centralized view and enhanced threat detection, investigation, and response across security layers like email, endpoints, servers, cloud workloads, and networks. By correlating data from these sources, it aims to improve threat detection, reduce alert fatigue, and enable faster, more effective responses to Security Incidents.