Cendyn™

Data Processing Agreement

Legal Department
July 1, 2025

GLOBAL DATA PROCESSING AGREEMENT

Updated on: July 1, 2025

This Cendyn Data Processing Agreement, including its exhibits and appendices ("**DPA**"), is entered into between Cendyn Group, LLC, a limited liability company incorporated under the laws of the State of Delaware, and its relevant Affiliates (collectively, "**Cendyn**") and Cendyn's counterparty ("**Customer**") to a Master Services Agreement ("**MSA**") or an order form or scope of work (together with the MSA, referred to as the "**Agreement**") to purchase Cendyn's Services (as defined below). Cendyn and Customer are referred to individually in this DPA as a "**Party**" and, collectively, the "**Parties**."

This DPA is effective when the last Party signs/assents to the Agreement (the "**DPA Effective Date**").

EXHIBITS AND APPENDICES

A. Exhibit A - Details of Processing;
B. Exhibit B - Jurisdiction Specific Terms;
C. Appendix I to Exhibit B – Supplementary Measures to the Standard Contractual Clauses; and
D. Exhibit C - Security Measures.

1. DEFINITIONS

1.1. In this DPA, the terms below (and their applicable derivations) mean:

(a) "**Affiliate**" is any entity within a controlled group of companies that directly or indirectly, through one or more intermediaries, is controlling, controlled by, or under common control with one of the Parties.

(b) "**Aggregate Customer Data**" is information processed by Cendyn or one of its Subprocessors (as defined below) on behalf of Customers that relates to a group or category of Data Subjects, from which individual identities have been removed, and that is not linked or reasonably linkable to any Data Subject or household, including via a device. Aggregate Customer Data is not Customer Personal Data.

(c) "**Applicable Data Protection Laws**" are laws and regulations applicable to the Processing of Customer Personal Data by the Services, including, but not limited to, the laws and regulations identified in **Exhibit B**, as may be amended from time to time.

(d) "**Customer Account Data**" is Personal Data that relates to Customer's relationship with Cendyn, including the names or contact information of individuals authorized by Customer to access Cendyn Services and/or account and billing information of individuals that Customer associates with its account.

(e) "**Customer Personal Data**" means any Personal Data that Cendyn or one of its Subprocessors Processes on Customer's behalf to provide the Services in accordance with the Agreement.

(f) "**Data Exporter**" and "**Data Importer**" have the same meanings assigned to them in **Exhibit A**.

(g) "**GDPR**" means the EU GDPR and UK GDPR as those terms are defined within **Exhibit B**.

(h) "**Jurisdiction Specific Terms**" means all terms applicable to the Processing of Personal Data that apply to the extent that Cendyn Processes via its Services Customer Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions identified in these terms. **Exhibit B** contains the Jurisdiction Specific Terms.

(i) "**Restricted Transfer**" means any transfer of Customer Personal Data protected by Applicable Data Protection Laws to a Third Country or an international organization in a Third Country (including data storage on foreign servers).

(j) "**SCCs**" or "**Standard Contractual Clauses**" means the model clauses for Restricted Transfers adopted from time to time by the relevant authorities of the jurisdictions indicated in **Exhibit B**, insofar as their use is approved by the relevant authorities as an appropriate mechanism or safeguard for Restricted Transfers.

(k) "**Services**" means the software and professional services and other activities carried out by or on behalf of Cendyn for Customer pursuant to the Agreement.

(l) "**Subprocessor**" means a direct Processor of a Processor.

1.2 The terms "**Controller**," "**Data Protection Impact Assessment**," "**Data Subject**," "**Member State**," "**Personal Data**," "**Personal Data Breach**," "**Processing**," "**Processor**," "**Rights of the Data Subjects**," "**Supervisory Authority**," and "**Third Country**" have the same meanings as under Applicable Data Protection Laws.

1.3 Capitalized terms that are used, but not defined, in the DPA have the meanings given to them in the Agreement.

2. SCOPE AND APPLICABILITY

2.1 **Duration.** This DPA begins on the DPA Effective Date and continues for as long as Cendyn Processes Customer Personal Data under the Agreement.

2.2 **Scope.** This DPA applies to the Processing of all Customer Personal Data.

3. PROCESSING OF CUSTOMER PERSONAL DATA

3.1 **Roles of the Parties**

(a) **Cendyn as a Processor of Customer Personal Data:** Regarding the Processing of Customer Personal Data by its Services, Cendyn is the Processor and Customer is the Controller.

(b) **Cendyn as a Controller of Customer Account Data:** Regarding the Processing of Customer Account Data, Cendyn is a Controller and Customer is a Controller. The Parties are independent and not joint Controllers. As an independent Controller, Cendyn processes Customer Account Data to: (i) manage the relationship with Customer; (ii) carry out Cendyn's core business operations, such as accounting and filing taxes; (iii) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (iv) verify identity; (v) comply with Cendyn's legal or regulatory obligation to retain subscriber data; and (vi) to comply with and as otherwise permitted by Applicable Data Protection Laws, this DPA, the Agreement, and Cendyn's Privacy Policy.

(c) Cendyn as a Controller of personal data provided by Customer through subscription to Cendyn's "Knowland Product" (as described in the MSA) with respect to "Readerboard Data" (as described in the MSA) . This Processing is covered under the Knowland Product Data Processing Agreement here. For all other processing activities for the Knowland Product, Cendyn acts as a processor.

3.2 Customer instructs Cendyn (and authorizes Cendyn to instruct each Subprocessor it engages) to Process Customer Personal Data and, in particular, transfer Customer Personal Data to any country or territory, only as reasonably necessary for the provision of the Services and consistent with the Agreement and this DPA.

3.3. Cendyn shall:

(a) comply with all Applicable Data Protection Laws in the Processing of Customer Personal Data;

(b) maintain all Customer Personal Data in strict confidence;

(c) only Process Customer Personal Data to perform the Services on behalf of Customer in accordance with the Agreement and this DPA and only on the documented instructions of the Customer, including with regard to Restricted Transfers, unless such Processing is required by the applicable laws to which Cendyn is subject, in which case Cendyn shall, to the extent permitted by Applicable Data Protection Laws, inform Customer of such requirement before Processing that Customer Personal Data;

(d) notify Customer where, in Cendyn's reasonable opinion, a Processing instruction given by the Customer may result in a violation of Applicable Data Protection Laws; and

(e) not attempt or be able to identify a Data Subject from Aggregate Customer Data.

3.4 Customer represents and warrants that it has all necessary rights to provide the Customer Personal Data to Cendyn for the purpose of Processing such data within the scope of this DPA and the Agreement. Within the scope of the Agreement and in its use of the Services, Customer shall be responsible for complying with the statutory requirements relating to data protection and privacy that apply to Customer, in particular regarding the disclosure and transfer of Customer Personal Data to Cendyn and Cendyn's Processing of Customer Personal Data.

4. SUBPROCESSORS

4.1 **Customer Consent for Subprocessors.** Customer consents to Cendyn using those Subprocessors already engaged as of the Effective Date of this DPA, and to engage or dismiss in the future any additional Subprocessors, as deemed necessary by Cendyn, provided that:

(a) in relation to future Subprocessors, Cendyn maintains an updated list of Subprocessors at https://www.cendyn.com/subprocessors_list/; and

(b) provides 30 days' prior notice via email and/or RSS feed notification to any of Customer's personnel who register (free of charge) to receive such notifications.

If Customer has not made a written objection to the new/additional Subprocessor within 14 days after Cendyn notifies Customer of the new/additional Subprocessor, Customer will be deemed to have consented to the additional Subprocessor.

4.2 **Objection to Subprocessors.** Customer may object, in writing, to the addition of a new Subprocessor appointed by Cendyn if Customer, in its reasonable discretion, believes that Cendyn's use of such new Subprocessor would result in a violation of Applicable Data Protection Laws, in which case the Parties agree to find a mutually agreeable alternative. If no such alternative is agreed within 90 days after Customer made its written objection, Customer will have the right to terminate, without penalty, only those Services for which Customer Personal Data would be Processed by the new Subprocessor against which the objection was raised.

4.3 **Requirements for Appointing Subprocessors.** With respect to each Subprocessor, Cendyn shall:

(a) ensure that the Subprocessor is capable of providing the level of protection and security for Customer Personal Data required by this DPA;

(b) restrict the Subprocessor's access to Customer Personal Data only to what is necessary to assist Cendyn in providing the Services; and

(c) ensure that the agreement between Cendyn and the Subprocessor is governed by a written contract that includes terms which offer at least the same level of protection for Customer Personal Data as those set out in this DPA, to the extent applicable, for the nature of the services provided by such Subprocessor.

4.4 Cendyn shall remain fully liable to Customer for the performance of its Subprocessors' obligations under this DPA.

5. RETURN OR DELETION OF CUSTOMER PERSONAL DATA

5.1 Cendyn shall provide Customer with the means, consistent with the way the Services are provided, to request the deletion of Customer Personal Data, with the exception of any Customer Personal Data that may be retained pursuant to applicable laws.

5.2 Following the cessation of Services, Cendyn shall return or destroy all Customer Personal Data (including copies) in its, or its Subprocessors', possession, custody, or control in accordance with the requirements of the Agreement, this DPA, and applicable laws, except for any Customer Personal Data that may be retained pursuant to applicable laws.

5.3 If Cendyn or its Subprocessor is legally obliged to store Customer Personal Data for a longer duration, Cendyn shall, if not prohibited by applicable law, inform Customer about the Customer Personal Data that will

be kept, the legal obligation, and the retention period. At the end of such retention period Cendyn shall delete the respective Customer Personal Data.

5.4 This Section 0 does not apply to Customer Personal Data that has been archived on back-up systems, which Customer Personal Data may be stored in Cendyn's back-up systems up to one month after the termination of the Services. Cendyn shall isolate and protect such archived Customer Personal Data from any further Processing, except to the extent required by applicable law.

5.5 Until Customer Personal Data is deleted or returned, Cendyn shall continue to ensure compliance with the DPA, and in particular the obligations described in this Section 5.

5.6 Upon request, Cendyn shall confirm compliance with the obligations described in this Section 0 in writing.

6. SECURITY OF CENDYN PROCESSING

6.1 In accordance with Applicable Data Protection Laws, Cendyn shall maintain and monitor a comprehensive, written information security program that contains technical and organizational measures to protect the security, confidentiality, and integrity of Customer Personal Data. *See* Exhibit C. The appropriate technical and organizational measures shall consider any applicable industry standards, the costs of implementation, the nature, scope, context and purposes of the Processing, and risks for the rights and freedoms of Data Subjects. Cendyn shall review and, as appropriate, revise its information security program once a year or sooner if there a material change in Cendyn's business practices that may reasonably implicate the security, confidentiality, or integrity of Customer Personal Data.

6.2 Cendyn shall ensure that its information security program covers all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones and other devices that Process or handle Customer Personal Data. Moreover, Cendyn shall ensure that its information security program includes industry-standard password protections, firewalls and anti-virus and malware protections to protect Customer Personal Data handled or stored on Cendyn's computer systems.

7. PERSONNEL

7.1 Cendyn shall take reasonable steps to ensure:

(a) the reliability of any of its employees, agents, or contractors who may have access to Customer Personal Data;

(b) that access to Customer Personal Data is strictly limited to those individuals who need to know or access it, as strictly necessary to fulfil the documented Processing instructions given to Cendyn by Customer or to comply with Applicable Data Protection Laws; and

(c) that all such individuals are subject to formal confidentiality undertakings, professional obligations of confidentiality, or statutory obligations of confidentiality.

8. GENERAL COOPERATION

8.1 **Rights of Data Subjects.** Cendyn will assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligations in responding to requests to exercise Rights of the Data Subjects under Applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Cendyn's provision of such assistance. With regard to the Rights of the Data Subjects within the scope of this Section 0, Cendyn shall:

(a) promptly notify Customer if it or any of its Subprocessors receive a request from a Data Subject with respect to Customer Personal Data;

(b) not respond to that request, except on the documented instructions of Customer or as required by Applicable Data Protection Laws, in which case Cendyn shall, to the extent permitted by

Applicable Data Protection Laws, inform Customer of such requirement before it responds to the request or directs its Subprocessor to respond; and

(c) promptly comply with any documented instructions from Customer regarding responding to a request to exercise Rights of a Data Subject.

8.2 **Requests Concerning Customer Personal Data to Cendyn.** If Cendyn directly receives a request related to any Customer Personal Data, Cendyn shall, where not legally prohibited from doing so, notify Customer as soon as reasonably practicable (no later than five business days), and shall not respond to any such requests unless this DPA, the Agreement, any applicable Statement of Work, or a written instruction from the Customer to Cendyn provides otherwise, or where Cendyn has a mandatory obligation under applicable law to respond directly. Cendyn shall reasonably cooperate with Customer to limit the scope of any disclosure to that which is legally necessary.

8.3 **Data Protection Impact Assessments and Prior Consultations.** Upon Customer's request, Cendyn agrees to provide Customer with relevant information and documentation, and to reasonably assist Customer in complying with its obligations with regard to any Data Protection Impact Assessments and prior consultations with Supervisory Authorities when required pursuant to Applicable Data Protection Laws, but in each such case solely with regard to Customer Personal Data Processed by, and taking into account the nature of the Processing and information available to, Cendyn and its Subprocessors.

8.4 **Cendyn's Assistance with Customer Security Obligations under Applicable Data Protection Laws.** Cendyn will provide reasonable assistance to Customer regarding Customer's compliance with its security obligations under Applicable Data Protection Law relevant to Cendyn's role in Processing the Customer Personal Data. In a situation where the requested level of assistance is repeated, not required by law, and/or burdensome for Cendyn, any such assistance will be provided at Customer's cost, and manpower hours will be calculated at Cendyn's then applicable professional services rate. For the avoidance of doubt, the parties agree that opening data centers in locations outside of where Cendyn already has established data centers is unduly burdensome.

9. PERSONAL DATA BREACHES

9.1 **Breach Response.** If Cendyn discovers, or is notified of, a Personal Data Breach affecting Customer Personal Data under its or its Subprocessors' control, Cendyn will:

(a) implement measures to stop the unauthorized access;

(b) secure the Customer Personal Data; and

(c) notify Customer in writing without undue delay.

9.2 **Breach Obligations.** Upon providing notice of a Personal Data Breach that impacts Customer Personal Data, Cendyn shall:

(a) describe to Customer in as much detail as reasonably possible: (i) the timing and nature of the Personal Data Breach; (ii) the impact of such Personal Data Breach upon Customer, and/or the impacted Data Subjects; (iii) the categories and approximate number of Personal Data records concerned and, where possible, the categories and approximate number of Data Subjects concerned; (iv) the corrective action taken or proposed to be taken by Cendyn to address the Personal Data Breach; and (v) the name and contact details of Cendyn's data protection officer or a contact point where more information can be obtained;

(b) provide and supplement the notifications as additional information becomes available;

(c) assist Customer in meeting its respective obligations pursuant to Applicable Data Protection Laws, including any obligations to notify Supervisory Authorities or Data Subjects of a Personal Data Breach; and

(d) use commercially reasonable efforts to investigate, mitigate, and remediate each such Personal Data Breach and prevent a recurrence of such Personal Data Breach.

9.3 **No acknowledgement of Fault.** Cendyn's notification of, response to, assistance with, or remedy of a Personal Data Breach under this Section will not be construed as an acknowledgement by Cendyn of any fault or liability with respect to the Personal Data Breach.

10. AUDIT RIGHTS

10.1 If, in accordance with Applicable Data Protection Laws, Customer is entitled to, and desires to, review Cendyn's compliance with the Applicable Data Protection Laws, Customer may request, and Cendyn will provide (subject to obligations of confidentiality and principles of reasonableness), relevant documentation or any relevant audit report Cendyn might have been issued with respect to its Services that involve the Processing of Customer Personal Data. If Customer, after having reviewed such documentation, still reasonably deems that it requires additional information, Cendyn may assist and make available to Customer, upon a written request and subject to obligations of confidentiality and principles of reasonableness, other information (excluding legal advice) and/or documentation necessary to demonstrate compliance with this DPA and the obligations pursuant to the Applicable Data Protection Laws. Cendyn shall allow for and contribute to reasonable audits by Customer or an auditor mandated by Customer (and subject to obligations of confidentiality) with regard to the Processing of the Customer Personal Data by Cendyn provided that such auditor is not a competitor of Cendyn. Cendyn shall provide the assistance described in this Section 10, so long as in Cendyn's reasonable opinion, such audits and the specific requests of Customer do not interfere with Cendyn's business operations or cause Cendyn to breach any legal or contractual obligation to which it is subject.

10.2 To the extent legally permitted, Customer shall reimburse Cendyn for any time expended for any such audit at Cendyn's then-current professional services rates.

11. JURISDICTION SPECIFIC TERMS. To the extent Cendyn Processes Customer Personal Data originating from or protected by Applicable Data Protection Laws in a jurisdiction listed in **Exhibit B**, then the terms and definitions specified in **Exhibit B** with respect to the applicable jurisdiction shall apply in addition to the terms of this DPA.

12. RESTRICTED TRANSFERS

12.1 Restricted Transfers of Customer Personal Data within this DPA's scope shall be conducted in accordance with **Exhibit B** and Applicable Data Protection Laws.

12.2 If the relevant authorities adopt a new version of SCCs as a lawful mechanism for Restricted Transfers in a jurisdiction governing the Processing of Customer Personal Data, the Parties are deemed to have agreed to the execution of the new version of the SCCs by signing this DPA, and, if necessary, Cendyn shall be entitled to update **Exhibit A** and **Exhibit B** (and their appendices) accordingly.

12.3 If an alternative transfer mechanism, such as Binding Corporate Rules, is adopted by Cendyn during the term of the Agreement (an "Alternative Mechanism"), and Cendyn notifies Customer that some or all Restricted Transfers can be conducted in compliance with Applicable Data Protection Laws pursuant to the Alternative Mechanism, the Parties will rely on the Alternative Mechanism instead of the transfer mechanisms in **Exhibit B** for Restricted Transfers to which the Alternative Mechanism applies.

12.4 In addition, Cendyn is certified to the EU-U.S., UK Extension to the EU-U.S., and Swiss-U.S. Data Privacy Frameworks and the commitments entailed. Cendyn agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Frameworks.

13. NO SALES OF CUSTOMER PERSONAL DATA BETWEEN CUSTOMER AND CENDYN. Cendyn confirms that it does not receive any Customer Personal Data as consideration for any Services or other items that Cendyn provides to Customer. Customer retains all rights and interests in Customer Personal Data. Customer agrees to

refrain from taking any action that would cause any transfers of Personal Data to or from Cendyn to qualify as selling Customer Personal Data under Applicable Data Protection Laws.

14. AMENDMENTS AND ONLINE HOSTING

14.1 Subject to this DPA, Cendyn may host the content of the exhibits and appendices of this DPA online, and further update the DPA, exhibits, and appendices in order to ensure that parties comply with Applicable Data Protection Laws.

14.2 The online DPA, exhibit, or appendix is considered by the parties as the latest version, and the parties agree that the online version takes precedence over the relevant DPA, exhibit, appendix originally agreed to by the parties.

15. RECORDKEEPING. Cendyn shall maintain all necessary documentation to evidence its compliance with this DPA for a period of two years after the expiration or termination of this DPA, or for such longer period as otherwise may be required by Applicable Data Protection Laws, whichever occurs latest.

16. GENERAL TERMS

16.1 **Governing Law.** This DPA is governed by and shall be construed in accordance with the laws of the state of Delaware. Each Party submits to the non-exclusive jurisdiction of the state and federal courts of Wilmington, Delaware.

16.2 **Notice.**

(a) Notice to Customer: Cendyn will send any notice made by Cendyn under this DPA to the data protection contact designated by the Customer.

(b) Notice to Cendyn: Any notice made by Customer will be provided in writing to the contact listed below.

Chief Legal Officer
301 Yamato Road, Suite 3194, Boca Raton, FL 33431, USA
Email: DPO@cendyn.com, with a copy to legal@cendyn.com

16.3 **Prior Existing Agreement.** This DPA supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations, and agreements, oral and written, with regard to this DPA's subject matter.

16.4 **Survival.** This DPA's termination or expiration shall not affect any rights or liabilities that accrued prior to such termination or expiry, or the coming into force, or continuance in force, of any term that is expressly or by implication intended to come into, or continue in force, on or after termination or expiry.

16.5 **No Waiver.** Delay in exercising, or failure to exercise, any right or remedy in connection with this DPA shall not operate as a waiver of that right or remedy.

16.6 **Severability.** If any part of this DPA is found to be legally invalid or unenforceable, it will be replaced with a valid provision that best reflects the original intent, and the rest of the DPA will remain in effect.

16.7 **Conflicts.** In the event of any conflict between the Agreement (including any annexes and appendices thereto) and this DPA, the provisions of this DPA shall prevail. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this DPA, the applicable Jurisdiction Specific Terms will prevail.

16.8 **Ambiguity.** Cendyn may amend this DPA without notice to or consent of Customer for the purposes of: (a) curing any ambiguity; (b) curing, correcting or supplementing any defective provision of the DPA; or (c) making

any other provisions with respect to matters or questions arising under this DPA; provided that such action shall not materially alter the DPA.

16.9 **Disclosure to Supervisory Authorities.** The Parties acknowledge that either Party may disclose this DPA and any relevant privacy provisions in the Agreement to Supervisory Authorities, or any other judicial or regulatory body, upon their request.

Exhibit A – Details of Processing

Subject Matter of Processing:	The subject matter of the Processing of Customer Personal Data pertains to the provision of the Services as detailed in the Agreement, provided that the Services are cloud-based and Cendyn has access or stores Customer Personal Data. For the avoidance of doubt, Services that do not involve Cendyn's Processing of Customer Personal Data (i.e., because all Customer Personal Data is stored by Customer and Cendyn does not have any access nor stores Customer Personal Data) are excluded from the scope of this DPA.
Nature and Purpose of Processing:	The purpose of the Processing of Customer Personal Data is to provide the Services detailed in the Agreement.
Duration of Processing:	The duration of the Processing of Customer Personal Data is subject to the terms of the Agreement and Section 0 of the DPA.
Categories of Data Subjects:	Depending on the Services provided to Customer, the categories of Data Subjects to whom the Personal Data relates may include: • past, existing, future customers of Customer (hotel guests, newsletter subscribers, customers of hotel restaurants, customers of casino hotels); • Customer's personnel; • Customer's leads; and • visitors to the Customer's website, provided by Cendyn as a part of the Services.
Categories of Personal Data:	Depending on the Services provided to Customer and the integrations that Customer elects, the categories of Customer Personal Data to be Processed may include, without limitation: • **Customers/clients of Customer (e.g., hotel guests, newsletter subscribers):** - Biographical information, including but not limited to first name, last name, gender. - Online identifiers, including but not limited to Customer ID, Source Guest ID, location data, IP addresses, device details, and cookie data. - Contact and address information, including but not limited to email address, reservation email and email status, home phone, address line, billing and delivery/shipping address, mobile phone, work phone, work extension, home phone, fax. - Accommodation information, including but not limited to company, property, number of stays, total nights, days since last stay, feedback provided. - Financial information, including but not limited to lifetime spend on the Customer's properties, transactional details, tax information, credit card information, and payment method. - Order details, including but not limited to order number, order date, order total, order status

	(pending/failed/cancelled/completed), and items purchased or added to cart/wish list. - Other information, including but not limited to photograph, reviews, and language. - Inferred information, including but not limited to information used to create a segment. • **Customer's personnel:** - Identifiers, including but not limited to Customer ID, account and username. - Biographical information, including but not limited to first name, last name, gender. - Contact information, including but not limited to: company, work email address, work phone, work extension, fax. - Log data, including but not limited to source and destination IP addresses, host name, user-ids, policy names, email addresses, URLs, date and time stamps, data volumes, activity and content. - Other information, including but not limited to job title.
Special Categories of Personal Data:	Special categories of Customer Personal Data: any categories of Customer Personal Data that Customer decides to Process in its use of the Services, including but not limited to data concerning health (such as food allergies or information relevant to hotel spa providers), sexual orientation (as may be inferred by combination of the civil status and bookings of double rooms), and data concerning an individual's religion (as may be inferred from food preferences).
Processing Activities:	Depending on the Services provided to Customer, the basic Processing operations to which the Personal Data will be subject include but are not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, alignment, or combination, blocking, erasure, and destruction.
Data Protection Officer:	**Cendyn:** VeraSafe, LLC 100 M Street S.E., Suite 600 Washington, D.C. 20003 USA Email: experts@verasafe.com Web: https://www.verasafe.com/about-verasafe/contact-us/ **Customer:** the information indicated in the Agreement (if any).

Article 27 EU Representative:	**Cendyn:** Serenata IntraWare GmbH Leopoldstr. 23 80802 München, Germany dpo@cendyn.com **Customer:** the Customer shall provide such information to Cendyn, if applicable, by emailing the following email address: dpo@cendyn.com OR the information indicated in the Agreement (if any).
Article 27 UK Representative:	**Cendyn:** Cendyn Limited Tindles Llp Medway House, Fudan Way Thornaby Stockton-On-Tees England TS17 6EN **Customer:** the Customer shall provide such information to Cendyn, if applicable, by emailing the following email address: dpo@cendyn.com OR the information indicated in the Agreement (if any).
Controllership Role:	As set out in Section 0 of the DPA, Customer acts as a Controller and Cendyn acts as a Processor for the Processing of Customer Personal Data.
Data Transfer Role:	**Cendyn:** Data Importer **Customer:** Data Exporter
Retention Criteria:	The retention period is the period during which the Services will be provided as described in the Agreement.
Frequency of Transfer:	The frequency of the transfer: continuous basis according to the terms of the Agreement.
Subject Matter, Nature, and Duration of Processing of Subprocessors:	Any transfer to Subprocessors will be only as strictly required to perform the Services pursuant to the Agreement. Upon request, Cendyn will provide to Customer a description of Processing for any Subprocessor(s), including the subject matter, nature, and duration of Processing.
Technical and Organizational Measures of Subprocessors:	When Cendyn engages a Subprocessor under the DPA, Cendyn and the Subprocessor must enter into an agreement with data protection terms substantially similar to those contained in the DPA. Cendyn must ensure that the agreement with each Subprocessor allows Cendyn to meet its respective obligations with respect to Customer. In addition to implementing technical and organizational measures to protect Customer Personal Data, Subprocessors must: • notify Cendyn in the event of a Personal Data Breach so that Cendyn may immediately notify Customer;

	• delete Customer Personal Data when instructed by Cendyn in accordance with Customer's instructions to Cendyn; • not engage additional Subprocessors without Cendyn's authorization; and • not process Customer Personal Data in a manner which conflicts with Customer's instructions to Cendyn.
Documented Instructions:	The following is deemed an instruction by Customer to Process Customer Personal Data: a) Processing in accordance with the Agreement. b) Processing initiated by Data Subjects in their use of the Services. c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. d) Asking Cendyn to receive or transfer data from/to a third party, which may include but it is not limited to Cendyn partners (for example, survey companies and reservation services providers). Processing necessary to provide the Services to Customer (which may include investigating security incidents and preventing spam or fraudulent activity, and detecting and preventing network exploits or abuse).

Exhibit B – Jurisdiction Specific Terms

1. European Economic Area

1.1. Definitions

(a) "**EEA**" means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.

(b) "**EEA Data Protection Laws**" means the EU GDPR and all laws and regulations of the EU and the EEA countries applicable to the Processing of Customer Personal Data.

(c) "**EU 2021 SCCs**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on 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.

(d) "**EU GDPR**" (as used in the DPA) means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as may be amended from time to time.

1.2. Restricted Transfers

(a) With regard to any Restricted Transfer subject to EEA Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. Cendyn's certification of the EU-U.S. Data Privacy Framework or any successors of the EU-U.S. Data Privacy Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the EU GDPR, as the case may be), provided that the Services are covered by the self-certification, if applicable;

ii. a valid adequacy decision adopted by the European Commission on the basis of Article 45 of the EU GDPR;

iii. the appropriate SCCs adopted by the European Commission from time to time; or

iv. any other lawful data transfer mechanism, as laid down in EEA Data Protection Laws.

1.3. Standard Contractual Clauses

(a) The DPA hereby incorporates by reference the SCCs.

(b) The Parties are deemed to have accepted, executed, and signed the SCCs where necessary in their entirety (including the annexures thereto).

(c) The Parties agree that any references to clauses, annexures, modules and choices within this Section shall be deemed to be the same as the cognate and corresponding references within any appropriate, updated SCCs, as may be applicable from time to time pursuant to the DPA.

(d) For the purposes of the EU 2021 SCCs and any substantially similar SCCs which may be adopted by the relevant authorities in the future:

i. The Parties agree to apply the following module:

(A) Module Two with respect to Controller-to-Processor Restricted Transfers.

ii. Clause 7: The Parties choose to include the optional docking clause. In particular, when Customer instructs Cendyn to integrate its services with a Cendyn partner, the Parties agree that the partner is authorized to join the EU 2021 SCCs concluded between Cendyn and Customers, as required by Clause 8.8 of the EU 2021 SCCs and in accordance with Clause 7 of the EU 2021 SCCs.

iii. Clause 9(a): The Parties choose option 2, "General Written Authorization," and the time period set forth in Section **Error! Reference source not found.** of the DPA (the procedures for designation and notification of new Subprocessors are set forth in more detail in Section 0 of the DPA).

iv. Clause 11: The Parties choose to include the optional language relating to the use of an independent dispute resolution body.

v. Clause 13 (Annex I.C):

(A) where Customer is a data exporter that is established in an EU Member State, the Supervisory Authority with responsibility for ensuring Customer's compliance with the GDPR shall be the Supervisory Authority for the EU Member State where Customer is incorporated as indicated in the Agreement, unless Customer indicates in writing that the Supervisory Authority shall be in a different EU Member State where Customer is established;

(B) where Customer is a data exporter not established in an EU Member State, but falls within the territorial scope of application of Article 3(2) of the GDPR, and has appointed a representative pursuant to Article 27(1) of the GDPR, then the country where Customer's EU Representative is registered (as indicated in either an order form or the signature page to the Agreement) shall be the competent supervisory authority; or

(C) where Customer is a data exporter that is not established in an EU Member State, the competent Supervisory Authority shall be in one of the EU Member States in which the data subjects are located (whose personal data is transferred in terms of the Standard Contractual Clauses. The competent Supervisory authority in such circumstances shall be the Supervisory Authority for the Republic of Ireland, unless Customer indicates that the Supervisory Authority shall be in a different EU Member State where the data subjects are located.

vi. Clause 17: The SCCs shall be governed by the laws of the Republic of Ireland.

vii. Clause 18: Any dispute arising from the SCCs shall be resolved by the courts of the Republic of Ireland.

viii. Annex I(A and B): The content of Annex I(A) and (B) is set forth in **Exhibit A**.

ix. Annex II: The content of Annex II is set forth in **Exhibit C**.

(e) The terms contained in **Appendix I to Exhibit B** to the DPA supplement the SCCs.

(f) In cases where the SCCs apply and there is a conflict between the terms of the DPA and the terms of the SCCs, the terms of the SCCs shall prevail with regard to the Restricted Transfer in question

2. Canada

When applicable, the Processing of Customer Personal Data shall be compliant with the Canadian Federal Personal Information Protection and Electronic Documents Act and any other applicable law, regulation, or decree of Canada pertaining to the protection of such information.

3. China

3.1. **Definitions**

(a) "**Applicable Chinese Data Protection Laws**" means the Cyber Security Law (**中**华人民 和国网络安全**法**), the Data Security Law (**数据安全法**) (when in force), the Personal Information Protection Law (**个人信息保**护**法**), the Provisions for the Online Protection of Children's Personal Information (**儿童个人信息网**络保护规定), the Measures for the Administration of Data Security (**数据安全管理**办法) (when in force), and the Measures for the Security Assessment for Cross-Border Transfer of Personal Information (**个人息出境安全**评估办法) (when in force).

(b) "**Controller**" includes "**Data processor**" as defined under Applicable Chinese Data Protection Laws.

(c) "**Data Subject**" includes "**Personal information subject**" as defined under Applicable Chinese Data Protection Laws.

4. India

When applicable, the Processing of Customer Personal Data shall be compliant with the Digital Personal Data protection Act, 2023, once effective, and any other applicable laws and regulations of India applicable to the Processing of Personal Data.

5. Switzerland

5.1. **Definitions**

(a) "**EU 2021 SCCs**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on 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.

(b) "**FDPIC**" means the Swiss Federal Data Protection and Information Commissioner.

(c) "**Swiss Data Protection Laws**" includes the Federal Act on Data Protection of 19 June 1992 ("**FADP**") and the Ordinance to the Federal Act on Data Protection.

5.2. **Restricted Transfers**

(a) With regard to any Restricted Transfer subject to Swiss Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. Cendyn's certification of the Swiss-U.S. Data Privacy Framework or any successor of the Swiss-U.S. Data Privacy Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the applicable Swiss Data Protection Laws, as the case may be), provided that the Services are covered by the self-certification, if applicable;

ii. a valid adequacy decision adopted by the FDPIC on the basis of Article 6 of the FADP;

iii. the appropriate SCCs adopted by the FDPIC from time to time; or

iv. any other lawful transfer mechanism, as laid down in Swiss Data Protection Laws.

5.3. **Standard Contractual Clauses**

(a) The DPA hereby incorporates by reference the EU 2021 SCCs, which have been adopted for use by the FDPIC with certain modifications. The Parties are deemed to have accepted, executed, and signed the EU 2021 SCCs where necessary in their entirety (including the annexures thereto).

(b) The Parties incorporate and adopt the EU 2021 SCCs for Restricted Transfers subject to Swiss Data Protection Laws in the same manner set forth in Section 1.3 of these Jurisdiction Specific Terms, subject to the following:

i. Clause 13 (Annex I.C): The competent authority shall be the FDPIC. Nothing about the Parties' designation of the competent Supervisory Authority shall be interpreted to preclude Data Subjects in Switzerland from applying to the FDPIC for relief.

ii. Clause 18: The Parties' selection of forum may not be construed as forbidding Data Subjects habitually resident in Switzerland from suing for their rights in Switzerland.

iii. References to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the FADP and the equivalent articles or sections therein, insofar as there are any Restricted Transfers subject to Swiss Data Protection Laws.

iv. The SCCs also protect the data of legal entities until the entry into force of the revised FADP.

(c) In cases where the SCCs apply and there is a conflict between the terms of the DPA and the terms of the SCCs, the terms of the SCCs shall prevail with regard to the Restricted Transfer in question.

6. United Kingdom

6.1. **Definitions**

(a) "**EU 2021 SCCs**" means the contractual clauses adopted by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on 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.

(b) "**UK Data Protection Laws**" includes the Data Protection Act 2018 and the UK GDPR.

(c) "**UK GDPR**" (as used in the DPA) means the United Kingdom General Data Protection Regulation, 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.

(d) "**UK ICO**" means the UK Information Commissioner's Office.

(e) "**UK Transfer Addendum**" means the International Data Transfer Addendum (version B1.0) to the European Union Commission's EU 2021 Standard Contractual Clauses issued pursuant to Section 119A(1) of the Data Protection Act 2018 and approved by the UK Parliament.

6.2. **Restricted Transfers**

(a) With regard to any Restricted Transfer subject to UK Data Protection Laws between the Parties, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. Cendyn's certification of the UK Extension to the EU-U.S. Data Privacy Framework or any successor of the UK Extension to the EU-U.S. Data Privacy Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the UK Data Protection Laws, as the case may be), provided that the services are covered by the self-certification, if applicable;

ii. a valid adequacy decision adopted pursuant to Article 45 of the UK GDPR;

iii. the appropriate SCCs adopted by the UK ICO from time to time (insofar as the Processing activities of the Data Importer are not subject to the UK GDPR by virtue of application of Article

3(2) of the UK GDPR; or

iv. any other lawful data transfer mechanism, as laid down in the UK Data Protection Laws.

6.3. **EU 2021 SCCs and UK Transfer Addendum**

(a) This DPA hereby incorporates by reference the EU 2021 SCCs which have been adopted for use by the UK ICO with certain modifications and the addition of the UK Transfer Addendum. The Parties are deemed to have accepted, executed, and signed the EU 2021 SCCs where necessary in their entirety (including the annexures thereto).

(b) For the purposes of the tables to the UK Transfer Addendum:

i. Table 1: The content of Table 1 is set forth in **Exhibit A**.

ii. Table 2: The content of Table 2 is incorporated and adopted as to Restricted Transfers subject to UK Data Protection Laws in exactly the same manner set forth in Section 1.3 of these Jurisdiction Specific Terms.

iii. Table 3: The content of Table 3 (Annexes 1A, 1B, II, and III) is set forth as follows:

i. Annex 1: The content of Annex 1 is set forth in **Exhibit A**.

ii. Annex II: The content of Annex II is set forth in **Exhibit C**.

iv. Table 4: The Parties agree that the Data Importer may terminate the UK Transfer Addendum.

(c) The Parties incorporate and adopt the EU 2021 SCCs as to Restricted Transfers subject to UK Data Protection Laws in exactly the same manner set forth in Section 1.3 of these Jurisdiction Specific Terms, subject to the following:

i. Clause 13 (Annex I.C): The competent authority shall be UK ICO.

ii. Clause 17: The EU 2021 SCCs, including the incorporated UK Transfer Addendum, shall be governed by the laws of England and Wales.

iii. Clause 18: Any dispute arising from the SCCs, or the incorporated UK Transfer Addendum, shall be resolved by the courts of England and Wales. A Data Subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.

(d) The terms contained in **Appendix I to Exhibit B** to the DPA supplements the SCCs.

(e) In cases where the SCCs, in conjunction with the UK Transfer Addendum, apply and there is a conflict between the terms of the DPA and the terms of the SCCs or UK Transfer Addendum, the terms of the UK Transfer Addendum shall prevail with regard to the Restricted Transfer in question.

7. Russia

7.1. **Definitions**

(a) "**Applicable Russian Data Protection Laws**" includes the Federal Law of 27 July 2006 N152-FZ on personal data, as may be amended from time to time;

(b) "**Controller**" includes "**Operator**" as defined under Applicable Russian Data Protection Laws;

(c) "**Data Subject**" includes "**Personal data subject**" as defined under Applicable Russian Data Protection Laws;

(d) "**Personal Data**" includes "**Personal Data**" as defined under Applicable Russian Data Protection Laws;

(e) "**Processing**" includes "**Personal data processing**" as defined under Applicable Russian Data Protection Laws;

(f) "**Russian Restricted Transfer**" (as used in this Section) includes any transfer of Personal Data (including data storage in foreign servers) which is undergoing Processing or is intended for Processing after transfer subject to Applicable Russian Data Protection Laws, to a Third Country (as defined below) or an international organization;

(g) "**Supervisory Authority**" includes the Roskomnadzor; and

(h) "**Third Country**" (as used in this Section) means a country other than the Russian Federation.

7.2. **Russian Restricted Transfers**

(a) With regard to any Russian Restricted Transfer from one Party to another within the scope of the Agreement, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. the Third Country's ratification of Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data;

ii. the inclusion of the Third Country in the list of other foreign states providing adequate protection of the data subjects' rights published by the Roskomnadzor;
iii. the Data Subject's consent to the Russian Restricted Transfer; or
iv. any other lawful basis, as laid down in the Applicable Russian Data Protection Laws, as the case may be.

(b) Customer confirms that it has obtained a valid consent (as defined under Applicable Russian Data Protection Laws) or identified an appropriate legal basis under Applicable Russian Data Protection Laws where necessary to Process Personal Data of each Data Subject and for the subsequent Processing by Cendyn and its sub-Processors.

(c) Customer has reviewed the security measures listed in **Exhibit C** to the DPA and agrees that they meet the standards required under Article 19(2) of the Federal Law of 27 July 2006 N 152-FZ on personal data.

8. Serbia

8.1. **Definitions**

(a) **"Applicable Serbian Data Protection Laws"** includes the Act of 9 November 2018 on Personal Data Protection (Official Gazette No. 87/18), as may be amended from time to time;

(b) "**Controller**" includes "**Rukovalac**" as defined under Applicable Serbian Data Protection Laws;

(c) "**Data Subject**" includes "**Lice na koje se podaci odnose**" as defined under Applicable Serbian Data Protection Laws;

(d) "**Personal Data**" includes "**Podatak o ličnosti**" as defined under Applicable Serbian Data Protection Laws;

(e) "**Processing**" includes "**Obrada podataka o ličnosti**" as defined under Applicable Serbian Data Protection Laws;

(f) "**Serbian Restricted Transfer**" (as used in this Section) includes any transfer of Personal Data (including data storage in foreign servers) which is undergoing Processing or is intended for Processing after transfer subject to Applicable Serbian Data Protection Laws, to a Third Country (as defined below) or an international organization;

(g) "**Serbian Standard Contractual Clauses**" (as used in this Section) means the Serbian Standard Contractual Clauses (Standardne Ugovorne Klauzule) adopted by the Supervisory Authority (as defined below) in Decision 5/2020 on the determination of standard contractual clauses in accordance with Applicable Serbian Data Protection Laws;

(h) "**Supervisory Authority**" includes the "Poverenik za informacije od javnog značaja I zaštitu podataka o ličnosti".

(i) "**Third Country**" (as used in this Section) means a country other than the Republic of Serbia.

8.2. **Serbian Restricted Transfers**

(a) With regard to any Serbian Restricted Transfer from one Party to another within the scope of the Agreement, one of the following transfer mechanisms shall apply, in the following order of precedence:
i. the Third Country's ratification of Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data;
ii. the inclusion of the Third Country in the list of foreign states, parts of their territories or one or more sectors of certain activities in those states and international organizations providing adequate protection of the data subjects' rights adopted by the Serbian government;
iii. the Serbian Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the Applicable Serbian Data Protection Laws, as the case may be); or
iv. any other lawful basis, as laid down in the Applicable Serbian Data Protection Laws, as the case may be.

8.3. **Serbian Standard Contractual Clauses**

(a) The DPA hereby incorporates by reference the Serbian Standard Contractual Clauses.

(b) The Parties are deemed to have accepted, executed, and signed the Serbian Standard Contractual Clauses where necessary in their entirety (including the appendices thereto).

(c) The Parties agree that any references to articles and appendices within this Section shall be deemed to be the same as the cognate and corresponding references within any appropriate,

updated SCCs as may be applicable from time to time pursuant to the DPA.

(d) For the purposes of the Serbian Standard Contractual Clauses and any substantially similar SCCs which may be adopted by the relevant authorities in the future:

i. Customer acts as the Controller and Cendyn acts as the Processor. The details of the Parties are as set out in the Agreement and this DPA.

ii. Article 12: The Serbian Standard Contractual Clauses will be applicable from the date when Cendyn commences to Process Personal Data protected by Applicable Serbian Data Protection Laws under the Agreement until the date when Cendyn ceases such Processing.

iii. Article 15: The Parties agree that disputes that arise under the Serbian Standard Contractual Clauses will be resolved by a competent court in the State of Florida, United States of America.

iv. Appendix 1: The details of Processing are set forth in **Exhibit A**.

v. Appendix 2: Cendyn shall only Process Personal Data on Customer's relevant documented instructions, as further described in Section 0 of the DPA.

vi. Appendix 3: A description of the technical and organizational security measures adopted by Cendyn are set forth in **Exhibit C**.

vii. Appendix 4: The Personal Data Breach Response period and corresponding obligations are set forth in Sections 0 and 0 of the DPA.

viii. Appendix 5: The Parties agree to the period specified under Section 4.30 of the DPA. A current list of Cendyn's Subprocessors is available at https://www.cendyn.com/subprocessors_list/.

ix. Appendix 6: Customer authorizes Cendyn to transfer Personal Data to Third Countries provided that the transfers are conducted in accordance with the provisions of the DPA. The countries where Cendyn and its Contacted Processors carry out their Processing operations includes, but is not limited to, the United States of America.

x. Appendix 7: The Parties agree to the procedure specified under Section 0 of the DPA.

(e) Where there is a conflict between the terms of the DPA and the terms of the Serbian Standard Contractual Clauses, the terms of the Serbian Standard Contractual Clauses shall control.

9. United States of America

9.1. **Applicability.** Wherever the Processing pursuant to the DPA falls within the scope of United States Data Protection Laws (defined below), the provisions of the DPA and this Section shall apply to such Processing.

9.2. **Definitions**

(a) **"United States Data Protection Laws"** include, individually and collectively, enacted state and federal laws, acts, and regulations of the United States of America that apply to the Processing of Personal Data, as may be amended from time to time. Such laws include, without limitation:

i. the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 *et seq.*), and the California Consumer Privacy Act Regulations, together with all implementing regulations;
ii. the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq., together with all implementing regulations;
iii. the Connecticut Act Concerning Data Privacy and Online Monitoring, Pub. Act No. 22015;
iv. the Texas Data Privacy and Securty Act, H.B. No. 4;
v. the Utah Consumer Privacy Act, Utah Code Ann. S 13-61-101 et seq.;
vi. the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-571 et seq.; and
vii. the Washington My Health My Data Act, Chapter 19.373 RCW.

(b) **"Personal Data Breach"** (as used in the DPA) includes "Breach of Security" and "Breach of the Security of the System" as defined under applicable United States Data Protection Laws.

(c) The terms "**Business Purpose**", "**Commercial Purpose**", "**Sell**", and "**Share"** shall have the same meanings as under applicable United States Data Protection Laws, and their cognate and corresponding terms shall be construed accordingly.

9.3. **Processing of Customer Personal Data**

(a) Customer discloses Customer Personal Data to Cendyn solely: (i) for the limited and specified Business Purposes set out in this DPA, including all its exhibits and appendices, particularly Section 9.3(b) below, and the Agreement; and (ii) to enable Cendyn to perform the Services under the Agreement.

(b) Cendyn Processes Customer Personal Data for the following Business Purposes:

i. performing Services on behalf of Customer, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying Customer Personal Data, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of Customer;
ii. auditing compliance with United States Data Protection Laws, as well as any other applicable standards or laws;
iii. ensuring the security and integrity of the Customer Personal Data;
iv. debugging to identify and repair errors that impair existing intended functionality of Cendyn products and Services;
v. short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a Consumer's current interaction with Cendyn's products or Services;
vi. providing advertising, marketing, and communication Services to Customer and its consumers;
vii. undertaking internal research for technological development and demonstration; and
viii. undertaking activities to verify or maintain the quality of Cendyn's Services and products provided to Customer, and to improve, upgrade, or enhance the Services and products provided to Customer.

(c) Cendyn shall:

i. refrain from Selling and Sharing Customer Personal Data;

ii. refrain from retaining, using, or disclosing Customer Personal Data: (i) for any purpose other than the Business Purpose(s) identified in this DPA, including all its exhibits and appendices, particularly Section 9.3(b) above, and the Agreement; (ii) for a Commercial Purpose other than the Business Purpose(s) identified in this DPA, including all its exhibits and appendices, particularly Section 9.3(b) above, and the Agreement; (iii) outside of the direct business relationship between Cendyn and the Customer; or (iv) as otherwise prohibited by United States Data Protection Laws.
iii. refrain from retaining, using, or disclosing Customer Personal Data except where permitted under the Agreement or United States Data Protection Laws;
iv. comply with its obligations under United States Data Protection Laws, including with respect to Customer Personal Data collected pursuant to the Agreement, and provide Customer Personal Data the same level of privacy protection required of Controllers under United States Data Protection Laws;
v. notify Customer if it makes a determination that it can no longer meet its obligations under United States Data Protection Laws;
vi. permit Customer to, upon reasonable notice of non-compliance with United States Data Protection Laws, take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data;
vii. not combine Customer Personal Data that it receives from Customer with the Personal Data that it receives from another Controller (or collects from its own interaction with Data Subjects), except if permitted by United States Data Protection Laws; and
viii. certify that it understands the restrictions set out in this Section 9 and will comply with them.

9.4. **Termination.** Upon termination of the Agreement, Cendyn shall, as soon as reasonably practicable, destroy all Personal Data it has Processed on behalf of Customer after the end of the provision of Services relating to the Processing and destroy all copies of the Personal Data unless applicable law requires or permits storage of such Personal Data.

10. Mexico

10.1. **Applicability.** Wherever the Processing pursuant to the DPA falls within the scope of the Federal Law on the Protection of Personal Data Held by Private Parties, and any corresponding decrees, regulations, or guidance, the provisions of this DPA and this Section shall apply to such Processing.

10.2. **General.** When acting as a Processor under the Federal Law on the Protection of Personal Data Held by Private Parties, Cendyn shall:

(a) Process Customer Personal Data only in accordance with Customer's instructions set forth in Section 0 and **Exhibit A** of the DPA;
(b) Process Customer Personal Data only to the extent necessary to provide the Services;
(c) implement security measures in accordance with Applicable Data Protection Laws and Section 0 of the DPA;
(d) maintain confidentiality regarding the Customer Personal Data Processed in accordance with the Agreement;
(e) delete all Customer Personal Data upon termination of the Agreement in accordance with Section 0 of the DPA; and
(f) only transfer Customer Personal Data to Subprocessors in accordance with Section 0 of the DPA.

11. Singapore

11.1. **Applicability.** Wherever the Processing pursuant to the DPA falls within the scope of Singapore's Personal Data Protection Act 2012, Personal Data Protection (Amendment) Bill 2020, Personal Data Protection Regulations 2021, and any corresponding decrees, regulations, or guidance, the provisions of the DPA and this Section shall apply to such Processing.

11.2. **Retention of Personal Data.** Cendyn shall not retain Customer Personal Data (or any documents or records containing Customer Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of the Agreement.

11.3. **Deletion or Return of Personal Data.** After returning or deleting Customer Personal Data pursuant to Section 0 of the DPA, Cendyn shall provide Customer with written confirmation that it no longer possesses any Customer Personal Data.

12. Macau

12.1. **Applicability.** Wherever the Processing pursuant to the DPA falls within the scope of Macau's Personal Data Protection Act (Act 8 of 2005), and any corresponding decrees, regulations, or guidance, the provisions of the DPA and this Section shall apply to such Processing.

12.2. **General.** Cendyn shall:

(a) implement security measures in accordance with Applicable Data Protection Laws and Section 0 of the DPA;
(b) Process Customer Personal Data only in accordance with Customer's instructions set forth in Section 0 of the DPA; and
(c) ensure that any Restricted Transfers of Customer Personal Data only takes place in accordance with the provisions of Applicable Data Protection Laws, in particular, Macau's Personal Data Protection Act.

13. Hong Kong

13.1. **Definitions.**

(a) "**Commissioner**" means the Office of the Privacy Commissioner for Personal Data.

(b) "**Controller**" includes "**Data User**" as defined under Hong Kong Data Protection Laws.
(c) "**Hong Kong Data Protection Laws**" includes the Personal Data (Privacy) Ordinance (Cap. 486), as may be amended from time to time, and any corresponding decrees, regulations, or guidance.
(d) "**Processor**" includes "**Data Processor**" as defined under Hong Kong Data Protection Laws.
(e) "**RMCs**" means the Recommended Model Clauses issued by the Commissioner for the transfer of Personal Data outside of Hong Kong pursuant to the Personal Data (Privacy) Ordinance (Cap. 486).

13.2. **General.** Cendyn shall:
(a) not retain Customer Personal Data (or any documents or records containing Customer Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of the Agreement; and
(b) implement security measures in accordance with Hong Kong Data Protection Laws and Section 0 of the DPA

13.3. **Restricted Transfers.**
(a) With regard to any Restricted Transfer between the Parties subject to Hong Kong Data Protection Laws, once of the following transfer mechanisms shall apply, in the following order of precedence:
i. a valid adequacy decision or determination issued by the Commissioner on the basis of Section 33(3) of the Personal Data (Privacy) Ordinance (Cap. 486);
ii. the appropriate RMCs adopted by the Commissioner from time to time; or
iii. any other lawful data transfer mechanism, as laid down in Hong Kong Data Protection Laws.

13.4. **Recommended Model Clauses.**
(a) The DPA hereby incorporates by reference the RMCs. The Parties are deemed to have accepted, executed, and signed the RMCs where necessary in their entirety (including the schedules thereto).
(b) The Parties agree that any references to clauses, appendices, and choices within this Section shall be deemed to be the same as the cognate and corresponding references within any appropriate, updated RMCs as may be applicable from time to time pursuant to the DPA.
(c) For the purposes of the RMCs and any substantially similar RMCs which may be adopted by the relevant authorities in the future:
i. the Parties agree to apply the Data User to Data Processor RMCs;
ii. the content of the Data Transfer Schedule to the RMCs is set out as follows:
i. Section 1 – Description of Transfer is set out in **Exhibit A** to this DPA;
ii. Section 2 – Sub-Processing is set out at https://www.cendyn.com/subprocessors_list/; and
iii. Section 3 – Security Measures is set out in **Exhibit C** to the DPA.

13.5. In cases where the RMCs apply and there is a conflict between the terms of the DPA and the terms of the RMCs, the terms of the RMCs shall prevail with regard to the Restricted Transfer in question.

.

Appendix I to Exhibit B -Supplementary Measures to the Standard Contractual Clauses

By this Appendix A (this "**Appendix**"), the Parties provide additional safeguards to and additional redress to the Data Subjects to whom Customer Personal Data relates. This Appendix supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses that may be applicable to the Restricted Transfer.

1. Applicability of this Appendix

This Appendix only applies with respect to Restricted Transfers where the terms of **Exhibit B** indicate it.

2. Definitions. For the purpose of interpreting this Appendix, the following terms shall have the meanings set out below:

2.1. "**EO 12333**" means the U.S. Executive Order 12333.

2.2. "**FISA**" means the U.S. Foreign Intelligence Surveillance Act.

2.3. "**Schrems II Judgment**" means the judgment of the European Court of Justice in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems.

3. Applicability of Surveillance Laws

3.1. Data Importer represents and warrants that, as of the DPA Effective Date, it has not received any national security orders of the type described in paragraphs 150-202 of the Schrems II Judgment.

3.2. Data Importer represents that it reasonably believes that it is not eligible to be required to provide information, facilities, or assistance of any type under FISA Section 702 because:

(a) no court has found the Data Importer to be an entity eligible to receive legal process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C. § 1881(b)(4) or (ii) an entity belonging to any of the categories of entities described within that definition; and

(b) if Data Importer were to be found eligible for FISA Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to UPSTREAM collection pursuant to FISA Section 702, as described in paragraphs 62 and 179 of the Schrems II Judgment.

3.3. EO 12333 does not provide the U.S. government the ability to order or demand Data Importer to provide assistance for the bulk collection of information and Data Importer shall take no action pursuant to EO 12333.

4. Backdoors

4.1. Data Importer certifies that:

(a) it has not purposefully created back doors or similar programming that could be used to access Data Importer's systems and/or Customer Personal Data subject to the SCCs;

(b) it has not purposefully created or changed its business processes in a manner that facilitates access to Customer Personal Data or systems; and

(c) national law or government policy does not require Data Importer to create or maintain back doors or to facilitate access to Customer Personal Data or system.

4.2. Data Exporter will be entitled to terminate the Agreement on short notice in cases in which Data Importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform Data Exporter once their existence comes to its knowledge.

5. Information about legal prohibitions. Data Importer will provide Data Exporter information about the legal prohibitions on Data Importer to provide information under this Appendix. Data Importer may choose the means to provide this information.

6. Additional Measures to Prevent Access. Notwithstanding the application of the security measures set forth in **Exhibit C** of the DPA, Data Importer will implement internal policies establishing that:

6.1. Data Importer must require an official, signed document issued pursuant to the applicable laws of the requesting third party before it will consider a request for access to Customer Personal Data;

6.2. Data Importer shall be notified upon receipt of each request or order for transferred Customer

Personal Data;

6.3. Data Importer shall scrutinize every request for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid;

6.4. if Data Importer is legally required to comply with an order, it will respond as narrowly as possible to the specific request; and

6.5. if Data Importer receives a request from public authorities to cooperate on a voluntary basis, Customer Personal Data transmitted in plain text may only be provided to public authorities with the express agreement of Data Exporter.

7. **Termination.** This Appendix shall automatically terminate with respect to the Processing of Customer Personal Data transferred in reliance of the SCCs if the Supervisory Authority or a competent regulator approves a different transfer mechanism that would be applicable to the Restricted Transfers covered by the SCCs (and if such mechanism applies only to some of the data transfers, this Appendix will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Appendix.

Exhibit C – Security Measures

A. Introduction and Objectives

Cendyn has implemented corporate information security practices and standards that are designed to safeguard Cendyn corporate environment and to address business objectives across information security, system and asset management, development, and governance.

These practices and standards are approved by Cendyn executive management and are periodically reviewed and updated where necessary. As such, this document and its objectives may change accordingly.

A-1 Technical Organization Measures

As stated in Article 32 of the GDPR under "Security of processing" it is required that "the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk".

Cendyn has structured this overview of its technical and organizational measures into the following categories:

- Organizational control
- Physical access control
- System access control
- Data access control
- System security control

A-2 Structure of the Document

This document is divided into three sections, first the document structure topics, second the Management initiatives and third the TOM-structured categories outlined above.

B. Applicability

B-1 Scope

This document outlines the security policies, practices, and controls in place for Cendyn platforms and applications.

B-2 Target Groups and Audiences

This document is mandatory directed to all employees of Cendyn. Employees are bound to the requirements based on this document. External parties and partners must also apply with these requirements.

B-3 Trust Commitment

Cendyn is committed to protecting the data that our customers have entrusted us with. Safeguarding the private information of individuals is also paramount. Cendyn warrants that it has in place physical, administrative safeguards and procedures to protect the confidentiality of all personal and confidential information of a customer. Cendyn maintains an Information Security Management System (ISMS) that addresses:

- User access and identity management
- Vulnerability management
- Change management
- Business continuity
- Physical security
- Network management
- Cryptography
- Human resources
- Incident response

All Cendyn employees with access to personal data are subject to confidentiality obligations which extend beyond cessation of the employee's employment with Cendyn.

B-4 Implementation

Data privacy documents are reviewed in yearly iterations or with required changes, whatever applies first. All data privacy related documents are reviewed and accepted by our DPO.

C. General Security Management

C-1 Risk Management

The Cendyn Risk Management program is divided into four phases:

- Risk Program executive-level authorization
  - Authorization and Support for beginning the risk management process.
  - Determine risk context (external and internal threats, existing controls, risk acceptance criteria).
- Risk identification
  - Identify the criticality of each asset group and impact of loss.
  - Determine risk owners and identify the risks applicable to each asset group.
  - Select the mitigation controls for each risk and their maturity level.
- Risk analysis and evaluation
  - Determine the level of risk, depending on the asset impact and risk likelihood.
- Risk treatment
  - Select the risk treatment options considering the risk assessment results and the risk acceptance criteria.

C-2 Data Residency

Cendyn's platforms are hosted and running on servers and hardware that we own and/or cloud technology we fully manage. For hardware we own: we house our equipment in a Tier 5 facility owned and managed by 365 Data Centers located at 3500NW Boca Raton Blvd, Building 900, Boca Raton, FL 33431. For Cloud technology, we leverage Azure, AWS, or GCP in the USA, EU, and APAC regions.

C-3 Audits and Certifications

Cendyn requires that 365 Data Center maintain SOC 2 audit standards.

Facility information can be reviewed here https://www.365datacenters.com/boca-raton-data-center/

Azure Compliance offerings https://docs.microsoft.com/en-us/azure/compliance/offerings/

AWS Compliance offerings https://aws.amazon.com/blogs/security/new-soc-1-2-and-3-reports-available-including-a-new-region-and-service-in-scope/

C-4 Security Policies and Procedures

Cendyn adheres to a comprehensive security policy framework. This framework includes standards for access control, HR processes, environmental/physical security, communications and network security, cryptography, software development, incident management, business continuity, vulnerability management, and data privacy. Cendyn's security policy framework is reviewed on a regular basis.

C-5 HR Policies

A Cendyn HR Specialist conducts background investigation for all new hires as well as existing personnel in critical roles or those who have access to sensitive information. The background check includes employment verification, educational and license or credential verification, criminal history, reference checks, and other pertinent information.

Employees are required to sign an employee contract, Code of Conduct, Employee Handbook, and participate in security awareness training.

New employee (Onboarding)

Cendyn follows the principle of least privilege. As new employees are onboarded only the required set of system permissions are granted. Authorization badges and/or keys are handed over by HR and/or the responsible department.

Termination of employee (Offboarding)

All permissions granted are terminated and login access is inactivated on the last day of employment or when their contract ends – whatever comes first. Access badges, keys, IT equipment and any other company assets are returned to HR and IT.

Job role and responsibilities changes

All permissions required for the previous role are rejected as the job change takes place.

Received access badges and keys must be authorized by HR on necessity for the new role. All permissions required for the new role and responsibility are granted by the time the previous permissions are taken.

C-6 Secure Supplier Evaluation

Cendyn conducts a review of service providers periodically. This review evaluates the security, privacy, service levels, and IT controls.

D. System Security Management

D-1 Data Classification and Handling

Cendyn's Asset Management policy defines a set of rules that help protect the confidentiality of information Cendyn processes. The rules set out in the policy describe several methods to protect data, such as controlling the access to sensitive and confidential information and protecting sensitive or confidential information. It is the responsibility of all Cendyn employees to classify their information and ensure appropriate measures to handle and protect data. The information lifecycle consists of:

- Labeling: Categorization of private, sensitive, public or unclassified
- Usage scope: Cendyn Internal or Client Data by application use
- Method of Transfer and encryption requirements
- Disposal

D-2 Change Management

Cendyn leverages documented processes and system-based Microsoft Operations Framework to ensure that all environmental changes are documented, tested, reviewed, and approved. A defined maintenance window is used for applying changes to systems in the environment, along with a communication plan informing all stakeholders of pending changes. System rollback procedures include backups before making any changes in addition to the regular nightly backups. The Change Management process involves four phases to deploy updates or fixes to the production environment.

- Communication
  - The technical owner proposing changes documents the change, including the requested change date, deployment owner and deployment manager.
- Deployment
  - The deployment steps are outlined with detailed steps to deploy changes to the application or environment.
- Test
  - The test plan describes the steps to take to confirm that the changes have been completed successfully. If the test plan fails, the technical owner determines whether to roll back the changes or continue troubleshooting.
- Rollback
  - The rollback plan describes the steps to revert the changes using a backup or snapshot created in the deployment phase.

Cendyn only makes changes to Cendyn Applications during scheduled maintenance windows.

D-3 Software Development Lifecycle

The Cendyn Software Development Lifecycle (SDLC) describes the processes in place to develop software in a secure manner. The SDLC model consists of several distinct stages including planning, design, building, testing, and deployment with security throughout the development process. Below is an outline of how we handle updates to Cendyn products.

- Planning and Requirements Analysis
  - Requirement analysis is performed by the senior members of the team with inputs from the customer and product subject matter expert. This information is then used to plan the basic project approach.
  - Planning for the quality assurance requirements and identification of the risks associated with the project is also done in the planning stage.

- Defining Requirements
    - Once the requirement analysis is done the next step is to clearly define and document the product requirements and get them approved from the Customer and/or the product manager. This is done through a BRD (Business Requirements Document) or other agile artifacts which consists of all the product requirements to be designed and developed during the project life cycle.
- Designing the change to product architecture (if required)
    - BRD is the reference for product architects to come out with the best architecture updates, if required. The design approach for the updated architecture is proposed and documented in a DDS – Design Document Specification.
    - This DDS is reviewed by all the important stakeholders and based on various parameters such as risk assessment, product robustness, design modularity, budget and time constraints, the best design approach is selected for the product.
    - A design approach clearly defines all the architectural modules of the product along with its communication and data flow representation with the external and third-party modules (if any). The internal design of all the modules of the proposed architecture should be clearly defined with the minutest of the details in DDS.
- Building or Developing the Product
    - In this stage of SDLC the actual development starts utilizing the Agile Model and product changes commence. The programming code is generated as per DDS during this stage.
    - Developers will follow Cendyn development guidelines.
- Testing the Product
    - While all stages have testing, this stage refers to the testing only stage of the product where product defects are reported, tracked, fixed and retested, until the product reaches the quality standards defined in the BRD.
- Deployment and Maintenance
    - Once the update is tested and ready to be deployed it is released formally in production with communication sent to clients.

D-4 Patch Management

Cendyn patch policy utilizes three tools to automate our patch management program. Each server is updated monthly.

- VMware provides scheduled snapshots of the server before a patch.
- Kaseya automates the approved patch utilizing a Patch Policy Membership that each server is assigned.
- PDQ is used to confirm that new patches have been installed.
- Cloud based systems provide for automated regular patching cycles.

D-5 Vulnerability Management

Cendyn corporate policy outlines the process and procedures to be followed when implementing a vulnerability management program. The policy is documented and divided into sections that identify, classify, remediate and mitigate vulnerabilities.

The core vulnerability management requirements:

- Documenting the roles and responsibilities associated with technical vulnerability management, including asset inventory, vulnerability monitoring, vulnerability risk assessment, remediation and mitigation, and any coordination responsibilities required.
- Performing vulnerability scanning to detect vulnerabilities.
- Classifying, remediating and mitigating the identified technical vulnerabilities.
- Implementing vulnerability management prior to enabling internet facing infrastructure or web applications.
- Implementing vulnerability management for major changes to the environment.
- Reporting status to management.

- Ensuring the vulnerability management procedure is an auditable process.

Vulnerability Scans are run monthly.

D-7 Penetration Test Management

Cendyn will perform penetration testing annually utilizing a trusted third-party vendor. Identified vulnerabilities will be addressed following the Cendyn vulnerability management program to identify, classify, remediate and mitigate vulnerabilities. Patch management is a component of the remediation plan within the vulnerability management policies. Patches are deployed to systems with the highest level of exposure and potential impact. All patches are deployed to development, QA, staging and finally production once all testing has been completed.

Targeted Vulnerability Scan and Penetration Testing Remediation Timeframes:

Critical	Fix or find remediation within two to four weeks from the date it was found
High	Fix or find remediation within two months from the date it was found
Medium	Fix or find remediation within 3 to 6 months from the date it was found
Low	At the discretion of the representative: no action, fix or find remediation within 6 to 12 months from the date it was found
Info	No action unless representative has a different reason/opinion

D-8 Incident Management

The Cendyn Incident Response Plan provides guidance for handling and communicating computer security incident responses at Cendyn. The Cendyn Incident Response Plan will be activated whenever a security incident occurs and guides the responses to all incidents whose severity is such that they could affect Cendyn's ability to do business, undermine its reputation or result in a financial impact to the company. It is the responsibility of every employee and contractor of Cendyn to immediately report any security incident to the Support Team.

Cendyn Support will work to resolve issues with malicious or unintentional alteration of data.

Intrusion Detection System

- Cendyn has implemented the Cisco FireSIGHT module at the ASA Firewalls which record all permitted and denied Intrusion Detection/Prevention events as determined by the Cisco Sourcefire IDS/IPS ruleset. The Cisco FireSIGHT module also does Application Firewall protections (i.e., SQL Injection, cross site scripting, etc.) for known and unknown vulnerabilities.
- Cendyn has also enabled the threat detection & protection to feature at the Cisco ASA perimeter firewalls to help mitigate DoS and other mass bot-net attacks. If the scanning threat rate is exceeded, then the ASA sends a system message, and shuns (blocks) the attacker for 30 minutes.
- We have a centralized log correlation via TrustedMetrics Services; alerts go out for suspicious activity at the network level and proper personnel take proper action and/or follow up. We also block IPs by monitoring load balancer logs to determine suspicious activity and if a pattern for non-trusted IPs is triggered; initiate the auto-shun (block) of such IPs at the Firewall.
- URl Filtering / URL Blocking: Cendyn has enabled the Cisco URL filtering feature at the firewall level to identify and control access to web (HTTP and HTTPS) traffic.
- FIM Alerts: changes to specific directories/shares, including new files, deleted files and modified files.

Response Team

Name/Team	Role/Title	Role and Responsibility of the Incident Response Team
Trusted Metrics	Cendyn Partner	Review of Logs (Security & Others). Always watching for anomalous behavior, so when things seem out of the ordinary, alerts go out.
Cendyn Support Team	Support Team	Responsible to audit alerts from multiple monitoring systems to analyze and validate a threat, error, etc. Once an issue is

		validated; escalate, triage & follow up until proper resolution is found.
IT Management	Senior Director, IT	Ensure Incident Response Plan is executed correctly. If there are any incidents, communicate with VP and executive teams.
IT Department	IT Team	Assist with investigation/ remediation of incident.
DEV Department	DEV Team per Product	Assist with investigation/ remediation of incident.
VPs	Company VPs	Correspond with clients as necessary and provide Support to VP of IT as needed.

The following documented response mechanisms serve as the Standard Operating Procedures for responding to any incident within the organization:

1. For any incident that has been detected, the Incident Response Team is to be immediately notified via Text Service and Communication Bridge opened.
2. The Incident Response Team is to formally assume control and to identify the threat and its severity to the organization's information systems.
3. In identifying the threat, the Incident Response Team is to specifically identify which resources, both internal and external, are at risk and which harmful processes are currently running on resources that have been identified as at risk.
4. The Incident Response Team is to determine whether the resources at risk (hardware, software, etc.) require physical or logical removal. Resources posing a significant threat to the continuity of the business are to be immediately removed or isolated, either physically or logically. Resources that may require physical or logical removal or isolation may include, but are not limited to, the following:
    - All IP addresses in use
    - Firewalls
    - Routers and switches
    - Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
    - Any enterprise-wide applications (CRM systems, etc.)
    - Remote access
    - Point-to-point secure data transmission methods used for data traversing back and forth on the network
    - Wireless networking or networks
    - Authentication servers (RADIUS)
    - Web servers
    - Proxy servers
    - File servers
    - Email servers
    - DNS servers
    - Operating systems
    - Databases
    - Applications
5. If the incident is identified as a DDoS attack, Cendyn should first contact R2 and then the ISP per the incident response plan.
6. If the incident has affected the PCI environment in any way, and has impacted the system components within this environment, Cendyn must immediately report the incident, its severity and other essential information to the major credit card payment brands (Ovations only).

7. Notify affected client contacts immediately after discovery of a breach, serious attempt to breach, unauthorized disclosure, or security incident which would compromise personally identifying information or other sensitive information such as payment card data. Do not notify or contact any customers directly without the authorization of the client.
8. If the incident has in any way resulted in a criminal matter that may be readily identified, Cendyn must immediately report it to law enforcement officials, such as the following:
    - Local law enforcement
    - The United States Secret Service (for credit card fraud)
    - The Federal Bureau of Investigation (FBI)
9. Investigating the incident is also a critical process within the Incident Response Plan. Proper investigative techniques are to include, but are not limited to, the following:
    - Understanding how the incident occurred and what led to the compromise.
    - Reviewing all necessary system documentation such as logs, audit trails, rule sets, configuration and hardening standards and all other supporting documentation.
    - Interviewing personnel as needed.
    - Examining any third-party providers and their respective products and services that are utilized within Cendyn's network architecture.
    - If warranted, a third-party resource for assisting in the investigation of the incident may be utilized (this will be done at the management's discretion).

Recovery from an Incident

Recovery procedures will include but are not limited to the following:

- Restoring systems from clean backups (a trusted source only).
- Completely rebuilding systems as needed and warranted.
- Replacing systems as needed (this includes all system components within the personally identifying information or cardholder data environment and any other IT resources deemed critical by Cendyn).
- Reconfiguring network security (stronger, more adaptive configuration and hardening rules) for all system components within the personally identifying information or cardholder data environment and any other IT resources deemed critical by Cendyn.

The recovery procedures will be commensurate with the incident that has occurred. This will be conducted on a case-by-case basis with all aspects of the recovery process fully documented.

Post-Incident Activities and Awareness

A formal and documented Root Cause Analysis (RCA) is to be compiled and given to management of Cendyn within an acceptable timeframe following the incident. The RCA must contain the following elements:

- What happened: a detailed description of the incident.
- Root cause: a description of the root cause.
- Resolution: steps taken for restoring affected systems.
- Timeline: timestamps from start to finish, including all important times from the incident.
- Impact: specific systems, accounts, and users affected by the challenge.
- Communication: reporting of the incident for all relevant third parties as needed.
- Lessons to Learn: A list of items, positive or learning touch points, from which Cendyn can take to improve systems and processes and hopefully eliminate the likelihood of future incidents.

All RCA documents will be stored in Salesforce and reviewed monthly by the INFOSEC Committee.

D-9 Disaster Recovery and Business Continuity

Cendyn participates in a corporate-wide program for business continuity planning. Critical business processes and the resources required to support those processes are inventoried. For each process and resource, an alternative is identified, such as a corresponding team at another site that can provide Support in the case of a business interruption until service is restored. Gaps are identified and addressed according to the documented process.

1. Organizational Controls

1-1 Contractual Base

Contract

Cendyn offers services on the basis of standardized contracts which fits our service design and the legal requirements.

The contracts are updated to incorporate any changes in the applicable law or in the general service design / technical functions. Changes are communicated transparently with the customer.

Terms & Conditions

The general Terms & Conditions define more specifically how the SaaS service is delivered, and which arrangements apply. Changes are communicated transparently with the customer.

Service Level Agreements

The SLAs define in a specific form the reaction and support levels on the basis of the severity of requests and escalation. Changes are communicated transparently with the customer.

Data Processing Addendum

The Cendyn DPA (available at https://www.cendyn.com/cendyn_customer_dpa/) defines in a standardized form the processing of customer personal data. Changes are communicated transparently to customers.

1-2 General Data Usage

Cendyn does not process PII without prior written consent of the owner. Cendyn requires customers to gain the consent for the submitted data which is specified in the contracts. Customers and or partners utilizing Cendyn services are required to obtain consent for the data to be processed.

1-3 Defined Overview of Sub-processors

Active service providing partners processing personal data on behalf of Cendyn, when Cendyn processes personal data on behalf of its customers, are added to a sub-processors list: https://www.cendyn.com/subprocessors_list/.

1-4 Security Awareness Training

All Cendyn employees are required to attend annual mandatory security awareness training. Training includes awareness of data privacy policies and issues, safe email and browsing habits, phishing and social engineering, and proper procedures for reporting security issues. Additionally, development staff are required to attend annual mandatory Secure Code Training

In addition to mandatory training, Cendyn employees receive weekly security notices outlining recent known threats on the internet and receive test phishing emails biweekly. Failure of the phishing test requires additional training.

2. Physical Controls

Cendyn has defined appropriate organizational (accompanying externals) and technical measures (key card token system) to protect against unauthorized physical access.

2-1 Definition of Security Areas

General

General areas can be accessed by all employees with their authorization badge.

The access is always bound to the exact location of employment.

Cendyn's sites are protected with electronic security, intrusion alarms, and fire detection equipment. Cendyn's data centers provide state-of-the-art innovative architectural and engineering methodologies and are housed in nondescript facilities as an added security measure.

Restricted

Restricted areas can only be accessed by authorized employees with separated access mechanisms (e.g., different authorization badges, keys).

365 Data Center physical access to the facility by requiring ID badges that are scanned for entry. Visitors require advance notice and proper ID and must enter through a reception area. They are required to sign in, and ID is matched to the advance reservation.

Additionally, physical access to the data centers is strictly controlled at building ingress points by professional security staff utilizing video surveillance and other electronic means like ID reader, magnetic or chip cards and door

locking mechanisms. Once within the data center, access is further restricted as Cendyn's equipment is contained within locked cabinets. Without the required key, nobody can access Cendyn's locked cabinets. All physical access to the premises is logged and audited routinely. Physical locations of Cendyn's data centers are carefully selected with co-location partners that meet or exceed the following standards:

- SSAE16 SOC1/2 – Type 2;
- PCI DSS Level 1; and
- Uptime Institute – Tier III.

In addition to requiring badges, all data centers require biometrics to gain physical access to the data center. The parking and surrounding areas of the data centers are inaccessible without a badge. All data centers have CCTV as well as fully auditable access logs. The data center racks themselves are also protected with locking front and rear doors. All cross connects and intra-cabinet cabling is completely shielded and secured.

3. System / Data Access Control

Cendyn has defined appropriate technical (e.g., login credentials) and organizational measures (e.g., access permissions through group policy based on AD groups) to protect against unauthorized system access.

3-1 Operational Measures

The following operational measures are in place to ensure technical and organizational security for user identification and authentication:

- Physical locations housing employees do not have direct network, VPN, etc. access to the server/data centers;
- Access to servers is controlled with client VPN, as well as maintenance of local workstation compliance leveraging Cendyn's configuration management tools;
- Client VPN is protected with MFA, UserID/Password and Duo;
- Server access once past all VPN controls, is then maintained with SSH keys; and
- Once in Cendyn's network, to access servers, a second VPN tunnel is established, to access production data. This is also protected with MFA but leverages a different UserID/Password combination.

3-2 Architecture and Data Segregation

Cendyn production and non-production environments are separated as required by policy. The systems exposed to the internet are kept isolated from internal systems that process and store data. The internal systems have several layers of protection including multiple firewall devices, access control lists, and intrusion detection systems. Access to network devices for management purposes are only provided through a logical and separate administration network.

Cendyn separates development, QA, staging, and production networks to reduce the risk of unauthorized access to, or changes in production. Segregation of duties is implemented to minimize the risk of negligence and to prevent intentional abuse of systems.

Cendyn customer data is separated by server and logical controls within the application.

Client data is retained per client request. All client data is routinely saved until the client is no longer contracted with Cendyn when it is purged and deleted. Some clients prefer a systematic purge and delete which can be set up and run to the client specifications.

3-3 Access Management

Cendyn corporate policies provide guidelines for managing access management, privileged access, and handling initial passwords.

Cendyn corporate policies provide guidelines to manage the identity lifecycle, access management, privileged access, handling of initial passwords, and identity de-registration:

Access Management

Formal access management processes and procedures are required to allocate the lowest level of system access rights required to allow the user to fulfill the assigned duties.

Privileged Access

Formal processes and procedures are required for the secure usage of privileged access. Management is responsible for the setup and operation of every user account with privileged access rights. The approval and usage of privileged accounts is based on need-to-use, need-to-handle, and least privilege principles. Users with privileged accounts are kept to a minimum. Multifactor authentication is enabled and implemented to get access to more critical infrastructure and/or secure environments.

Product Access – Hotel Users

Admin Role has single property access to all functionality plus access to add/remove users and to view all users and proposals.

Non-Admin Role has access to all functionality for themselves only.

Handling of Initial Passwords

A formal password provisioning procedure is required to securely allocate initial passwords to users. Every Cendyn user account must have a unique initial password assigned to the user and must be communicated to the user in a secure manner. The initial password is only temporary and must be changed by the user upon first logon.

Admin user password security

Password requirements:

- Cannot be all digits.
- Cannot be all lowercase letters.
- Cannot be all Uppercase letters.
- Cannot be all Mix letters.
- Cannot be all Uppercase letters (this includes numbers).
- Cannot be all lowercase letters (this includes numbers).
- Must be more than 6 characters.
- Must be less than 15 characters.
- Cannot contain ‘password’, including leet variants.
- Cannot contain ‘qwerty’, including leet variants.
- Cannot be simple word with 123…
- Cannot be simple word with 123 or 1234… prepended.
- Cannot be simple word with 1’s appended.
- Cannot be simple word with 1’s prepended.
- User is locked out after five incorrect attempts.

Cendyn corporate policies define security mechanism requirements for accessing Cendyn systems and applications to avoid or impede unauthorized access. The policy outlines the controls in place including secure log-on procedures, password management systems, use of privileged utility programs, and access control to program source code.

All usernames and passwords are created and altered from generally recognized principles and no username is reused within a period of at least 4 months since the username was last in use. If at any time an employee has not used their username within a period of 3 months, the username will automatically be suspended. Cendyn employees with access to the IT solution are covered by a strict password policy. All system access passwords must be unique from the user's last 24 passwords and must be changed at least every 3 months.

Secure log-on procedures

Systems and technical owners implement and manage secure log-on procedures/measures to support control and minimize access to Cendyn systems. Examples would include:

- The number of unsuccessful log-on attempts is limited to a maximum of five attempts.
- The passwords are not transmitted in plain text over any network.

Password Management Systems

- The password procedure enforces complex passwords.

Access control to program source code

- Technical owners implement and manage procedures for access to the source code to prevent the introduction of unauthorized functionality and to avoid unintentional changes, access to the program source code.
- All changes to the application are strictly controlled and follow the appropriate change process.
- Access to the source code and associated items (e.g., designs, specifications, verification plans, validation plans, etc.), are granted on a need-to-know basis and strictly controlled.

The source code is centrally managed, and access is logged.

Disclosure Control

Data transfers occur via a secure VPN or over a company-owned network. When Cendyn employees access Cendyn systems, connections are secured through encryption. Any access to Cendyn's IT systems requires that the employees register a username and a password. All data transfers are audited and must be business justified and limited to the minimum necessary data.

Input Control

Cendyn employs measures to log the username, time, type of application, and the person that data is concerning, to ensure all access to personal data is kept on record. Cendyn maintains logs for a minimum of 6 months, which are deleted after a maximum of 7 months. All system, security, network, and application logs are streamed in real time to an outsourced SIEM. This SIEM alerts on all predefined incidents/patterns with an SLA of 15 minutes.

Availability Control

Cendyn secures stored data through the regularly scheduled backup of stored data. The backup is conducted as a mix of full backup and incremental backup. Cendyn regularly conducts tests of previously completed backups to ensure that the backup routines function as intended. For safety reasons, critical backups are also duplicated and stored in another data center from the same provider in the same country and region. For systems that are hosted in the cloud, backups are taken and stored by the cloud provider automatically.

Cendyn's data centers electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Pegasus´s business continuity procedures include backup copies at alternate data centers, with pre-configured servers available if operations need to be shifted between data centers.

Climate control is required to maintain a constant operating temperature for the servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. Electrical, mechanical, and life support systems and equipment are monitored so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

4. System Security Controls

4-1 Cryptography

Cendyn corporate policies define the requirements for cryptographic algorithms, protocols, and handling the underlying cryptographic keys (generation, use, protection, selection, and lifetime). The requirements are based on industry best practices. Various methods are being utilized to secure data at rest and in transit.

Cendyn products provide a minimum of TLS 1.2 to encrypt data in motion and industry-standard AES 256 or higher for data at rest. Regarding data backup, we use Dell/EMC SAN devices in our 100% Virtual Infrastructure where data is stored, and these devices natively run (AES-XTS) 256 encryption.

4-2 Anti Malware

The Cendyn corporate policy framework defines procedures and controls for handling the protection of systems from malware. Cendyn systems are protected to prevent, detect and remove malware and ensure that users are aware of the risks that might arise.

Preventive Measures

Cendyn employees are made aware of the risks that malware might cause and which preventive measures they can take via annual training and weekly security updates. Examples of potential risks include:

- Installing software on Cendyn managed software.
- Downloading files.
- Attachments to suspicious emails.
- Use of removable media.
- Reporting suspicious or possible malware infection.
- USB Drop Tests.

Detective Measures

Cendyn systems are automatically and regularly inspected for malware. At least the following elements are inspected:

- Emails and attachments transferred via Cendyn email systems before use.
- Files received by any medium, before use.
- Content published on the Intranet and Internet.
- Access to websites.
- All data, software, and other files from removable storage.

Logging and Monitoring

Cendyn uses a combination of tools to monitor our Applications, Availability, Logs and Performance. We have procedures and tools for the following activities:

- Infrastructure performance and monitoring.
- Application code and errors monitoring.
- Site monitoring and availability metrics.
- Security events correlation using a SIEM tool.