DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**DPA**") is incorporated by reference into, and forms an integral part of, the Master Sales, Service, and License Agreement ("**Service Agreement**") between **Customer** and **Janus International Group LLC,** 135 Janus International Boulevard, Temple, Georgia 30179, United States, on behalf of itself and its Affiliates as set forth in Appendix 2 ("**Supplier**"), each a "**Party**" and collectively, the "**Parties**." By executing the Service Agreement, the Parties acknowledge that this DPA is legally binding and enforceable as of its execution date (the "**Agreement Date**"), without requiring a separate signature on this DPA.

RECITALS:

A Customer and Supplier have entered into a Service Agreement under which Supplier provides storage facility-related mobile applications and associated services to Customer (the "**Services**").

B In providing the Services, Supplier Processes Personal Data, and this DPA governs such Processing as a supplement to the Service Agreement.

C Supplier may act as a Processor or Subprocessor when Processing Personal Data on behalf of Customer, which determines the purposes and means of such Processing, and may also act as an independent Data Controller for the limited purposes set forth in Appendix 1.

D If any provision of the Service Agreement conflicts with this DPA, the terms of this DPA shall prevail to the extent that the latter provides greater protection for Personal Data.

2. DEFINITIONS

In this DPA, the following terms have the following meanings:

"**Affiliate**" means any entity that now or in the future controls, is controlled by, or is under common control with Supplier (with "control" defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of another entity, whether through the ownership of voting securities, by contract, or otherwise), and that Supplier has expressly designated as covered under this DPA in Appendix 2.

"**Applicable Data Protection Laws**" means all data protection, privacy, and security laws and regulations applicable, and only to the extent required and applicable, to the Processing of Personal Data under this DPA, including, without limitation, General Data Protection Regulation ("**GDPR**") Regulation (EU) 2016/679; the UK General Data Protection Regulation ("**UK GDPR**"), as implemented by the UK Data Protection Act 2018; the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA**"); the Swiss Federal Act on Data Protection, RS 235.1 ("**Swiss FADP**"), as amended from time to time; and Quebec's Act to Modernize Legislative Provisions as Regards the Protection of Personal Information S.Q. 2021, c. 25. ("**Law 25**"), the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") and any other Applicable Laws that regulate data protection, privacy, or the Processing of Personal Data in connection with the Service Agreement.

"**Applicable Laws**" means all laws, regulations, statutes, directives, and other legal requirements, including but not limited to Applicable Data Protection Laws, that govern or otherwise impose obligations on the Parties with respect to the Processing of Personal Data.

This includes laws related to security, consumer protection, financial regulations, electronic communications, fraud prevention, law enforcement requests, regulatory requirements, and any other legal obligations that supersede or supplement Applicable Data Protection Laws.

"**Controller**" means the Party that alone determines the purposes and means of the Processing of Personal Data, including any role equivalent to a Controller or Business as defined under Applicable Data Protection Laws.

"Data Subject" means any identified or identifiable natural person whose Personal Data is Processed under this DPA, including consumers, tenants, employees, personnel, and authorized users of the Services. Where required by Applicable Data Protection Laws, Data Subject also includes households and individuals authorized to act on their behalf.

"End User" means any individual who accesses or uses the Nokē® Smart Entry Software, including Customer's tenants, individuals with whom Customer's tenants share their Nokē® Smart Entry Software digital key(s), Customer personnel, and authorized third-party contractors.

"**Instructions**" means (i) the obligations and requirements set forth in this DPA and the Service Agreement, and (ii) any additional written instructions that Customer provides to Supplier regarding the Processing of Personal Data, provided that such instructions are consistent with the terms of the Service Agreement and Applicable Laws.

"**Personal Data**" means any information relating to an identified or identifiable natural person, as provided to, accessed, collected, or Processed by Supplier in connection with the Service Agreement, including "Personal Information" or any equivalent term as defined under Applicable Data Protection Laws.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"**Processing**" means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, storage, retrieval, disclosure, modification, structuring, and deletion.

"Processor" means Supplier when it Processes Personal Data on behalf of Customer or another Processor, including roles equivalent to a Processor, Subprocessor, or Service Provider under Applicable Data Protection Laws. Where Supplier acts as a Subprocessor, the obligations applicable to Processors under this DPA shall apply to Supplier in its role as a Subprocessor, unless explicitly stated otherwise.

"**Quebec Transfer Clauses"** means the contractual clauses required for cross-border transfers of Personal Data under Section 17 of Law 25, as prescribed by the Commission d'accès à l'information du Québec (CAI) or any successor clauses recognized under applicable Quebec privacy law.

"**Sale,**" "**Sell,**" "**Share,**" and "**Sharing**" shall each be ascribed the meaning set forth in the Applicable Data Protection Laws.

"**Standard Contractual Clauses**" or "**SCCs**" means the contractual clauses for international transfers of Personal Data annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, in force 27 June 2021, and as may be amended or replaced by the European

Commission from time to time.

"**Subprocessor**" means any third party, including Supplier when acting in that capacity, engaged to Process Personal Data on behalf of a Processor in fulfilling its obligations under the Service Agreement. This includes circumstances where Supplier Processes Personal Data on behalf of another Processor as a Subprocessor. When Supplier acts as a Processor, Subprocessor does not include Supplier's own personnel or individual contractors. The list of Subprocessors engaged by Supplier in connection with the Service Agreement is provided in Appendix 1, Annex 3.

"**Swiss Addendum**" means the Standard Contractual Clauses as recognized under the Swiss FADP, including any necessary modifications to align with Swiss law, as issued or endorsed by the Swiss Federal Data Protection and Information Commissioner (FDPIC) and as may be amended or replaced by the Swiss government or competent regulatory authorities from time to time.

"UK Addendum" means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner's Office under Section 119A(1) of the Data Protection Act 2018, in force as of 21 March 2022, and as amended or replaced from time to time by the UK Information Commissioner's Office and/or the Secretary of State.

3. CUSTOMER OBLIGATIONS

3.1 Customer is solely responsible for ensuring that its collection, use, and disclosure of Personal Data comply with Applicable Data Protection Laws. This includes (i) ensuring the accuracy, quality, and lawfulness of Personal Data; (ii) obtaining any necessary legal basis for Processing; and (iii) providing lawful instructions for Processing. Supplier shall have no obligation to verify these factors unless expressly required by Applicable Data Protection Laws.

4. SUPPLIER OBLIGATIONS AS A PROCESSOR

4.1 Compliance with Instructions

To the extent Supplier will Process Personal Data as a Processor on behalf of Customer, Supplier shall Process Personal Data only in accordance with Customer's Instructions under this DPA and the Service Agreement, provided such Instructions are commercially reasonable, technically feasible, and consistent with Applicable Data Protection Laws.

4.2 Legal Obligations

Supplier may Process Personal Data as necessary to comply with its obligations under Applicable Laws, including but not limited to Applicable Data Protection Laws. Supplier shall not be required to follow any Instructions that conflict with this DPA, the Service Agreement, or Applicable Laws.

4.3 Notification of Potential Violations

If Supplier determines or reasonably suspects that a Customer Instruction may violate Applicable Laws, it shall notify Customer without undue delay, unless prohibited by law.

4.4 **Supplier Commitments as a Processor**

In acting as Processor, the Supplier shall:

4.4.1 Maintain processing records and, upon reasonable notice, provide documentation demonstrating compliance, subject to Section 6.3 of this DPA and confidentiality and security constraints;

4.4.2 Limit access to Customer's Personal Data to only those employees, agents, or Subprocessors who require it to perform the Services and impose appropriate confidentiality obligations consistent with Applicable Data Protection Laws;

4.4.3 Use reasonable efforts to notify Customer if a supervisory or other regulatory authority requests access to Personal Data and unless required by Applicable Laws, shall use reasonable efforts not to provide such access without first notifying Customer, except where prohibited;

4.4.4 Upon termination or expiration of the Service Agreement, Supplier shall, unless otherwise instructed by Customer in writing within thirty (30) days, (i) securely return all Personal Data, or (ii) securely erase all Customer Personal Data in its possession, unless retention is required by Applicable Laws. Supplier will use commercially reasonable efforts to require its Subprocessors to enter into written agreements containing obligations that are substantially similar to, and no less protective than, those set out in this DPA.

4.4.5 Notwithstanding the foregoing, Personal Data stored in non-production backup or archival systems shall be erased in accordance with Supplier’s documented retention schedule, provided such data remains subject to the security, confidentiality, and access controls set forth in this DPA.

4.5 **Assistance with Compliance**

Taking into account the nature of Processing and the information available to Supplier, Supplier shall provide reasonable assistance to Customer by:

4.5.1 Forwarding Data Subject rights requests under Applicable Data Protection Laws to Customer and, unless otherwise required by Applicable Laws or expressly instructed by Customer, not Processing Personal Data in connection with such requests except as necessary for verification and authentication;

4.5.2 Providing reasonable assistance in meeting security, breach notification, impact assessment, and regulatory consultation obligations under Applicable Data Protection Laws; and

4.5.3 Assistance beyond Supplier’s standard compliance obligations, including extensive assistance with Data Subject rights requests, impact assessments, or regulatory consultations, may be subject to reasonable fees, unless otherwise required by Applicable Data Protection Laws.

4.6 **CCPA Obligations**

The Parties acknowledge that when Supplier Processes Personal Data of California residents on behalf of Customer, it acts as a Service Provider, and Customer acts as a Business under the CCPA. The disclosure of such Personal Data does not constitute, and is not intended to constitute, a Sale or Sharing under the CCPA. Any exchange of valuable consideration between the Parties is solely for the provision of Services as defined in the Service Agreement and not for the disclosure of Personal Data.

4.6.1 **Supplier Obligations as a Service Provider**

When acting as a Service Provider, Supplier shall:

4.6.1.1 Not Process Personal Data for any purpose other than performing the Services or as required by Applicable Laws, nor Process outside the direct business relationship between Supplier and Customer unless expressly permitted by Applicable Laws;

4.6.1.2 Not Sell or Share Personal Data, except as necessary to fulfill its obligations under the Service Agreement;

4.6.1.3 Not combine Personal Data with personal information from other sources except as permitted under the CCPA for a defined business purpose, including where necessary for security, fraud prevention, or compliance with Applicable Laws;

4.6.1.4 At Customer's reasonable, written request, restrict or cease any unauthorized Processing of Personal Data and allow Customer to assess and remediate such Processing subject to Section 6.3 of this DPA, unless prohibited by Applicable Laws;

4.6.1.5 If Supplier determines or receives credible evidence that its Processing may violate the CCPA, it shall promptly notify Customer and cooperate in good faith to resolve the issue. Upon such notification, and subject to Section 6.3 (Audit Rights), the Customer may take reasonable and appropriate steps to assess and address the potential non-compliance, including requesting additional information and discussing remedial measures. Upon Customer's reasonable, written request, Supplier shall take commercially reasonable steps to cease or modify such Processing unless prohibited by Applicable Laws.

5. SUPPLIER OBLIGATIONS AS A CONTROLLER

5.1 When acting as a Controller, Supplier acknowledges its responsibilities under Applicable Data Protection Laws.

5.2 When acting as a Controller, Supplier Processes Personal Data that is automatically generated through Customer's use of the Services, including log data, credentialing, access patterns, and diagnostic or operational insights ("**Usage Data**"). Supplier shall only process such data for its own legitimate interests, such as product improvement, development, analytics, and internal reporting.

5.3 Customer acknowledges that Supplier may use anonymized and aggregated data, provided that no such use shall involve the re-identification or further processing of Personal Data under this DPA.

5.4 Supplier retains all rights, title, and interest in Usage Data and anonymized, de-identified, and aggregated data. While Usage Data may include Personal Data, anonymized and aggregated data is by definition not Personal Data under Applicable Data Protection Laws and falls outside the DPA privacy obligations. Supplier may use both for legitimate business purposes, including improving, developing, and securing the Services, and will make no attempt to re-identify anonymized or aggregated data.

6. SECURITY MEASURES

6.1 Obligation to Implement Technical and Organisational Measures to Protect Personal Data

6.1.1 Supplier shall implement and maintain technical and organizational security measures appropriate to the risk and consistent with Applicable Data Protection Laws, including those set out in Annex II, which applies to all Processing under this DPA.

6.1.2 Subject to Section 6.3, upon Customer's reasonable request, Supplier shall provide relevant information and commercially reasonable assistance to support Customer's compliance with security obligations under Applicable Data Protection Laws, including data protection impact assessments and consultations with supervisory authorities where required.

6.2 Personal Data Breach

6.2.1 Notify Customer without undue delay upon becoming aware of a Personal Data Breach and provide timely updates as additional relevant details become available.

6.2.2 Supplier shall, where available, provide the following details to Customer regarding the Personal Data Breach:
(i) The nature of the breach, including the categories and estimated number of affected Data Subjects and records; and
(ii) the likely consequences of the breach, if known.

6.2.3 If full details are unavailable at the time of notification, Supplier may provide updates in phases without undue delay. Such notification is provided to comply with Applicable Data Protection Laws and shall not be construed as an admission of fault, liability, or wrongdoing by Supplier.

6.3 Audit Rights and Compliance Verification

6.3.1 Supplier shall permit and contribute to one (1) reasonable audit per calendar year subject to Section 6.3.2, conducted by Customer or an independent third-party auditor approved by Supplier, unless otherwise required by Applicable Data Protection Laws. Audits require thirty (30) days' notice and shall not unreasonably disrupt Supplier's operations.

6.3.2 Supplier maintains industry-recognized security certifications (e.g., SOC 2) and will make available the most recent audit reports upon request. Where Supplier holds such certifications, additional direct audits shall be permitted only upon demonstrable evidence of material non-compliance.

6.3.3 Customer shall bear the costs of any audit conducted under Section 6.3.1, including third-party auditor fees. If an audit identifies non-compliance by Supplier, Supplier shall remediate the issue within a reasonable timeframe. The Parties shall discuss in good faith any cost-sharing for remediation efforts caused by Supplier's non-compliance with this DPA; however, nothing in this Section shall obligate Supplier to subsidize or reimburse Customer's audit costs, unless such reimbursement is required by Applicable Data Protection Laws. All audits must adhere to Supplier's security, confidentiality, and access protocols as outlined in Section 6.3.2.

7. USE OF SUB-PROCESSORS

7.1 Customer hereby grants Supplier a general authorization to engage Subprocessors to Process Personal Data on behalf of Supplier, subject to the terms of this Section 7. Supplier shall enter into a written agreement with each Subprocessor that imposes obligations equivalent to those set forth in this DPA, including those required under Applicable Data Protection Laws.

7.2 As of the Agreement Date, all authorized Subprocessors are listed in Appendix 1, Annex 3. Supplier also maintains a publicly available Subprocessor list at www.janusintl.com/subprocessors ("**Subprocessor List**"), which will be updated periodically to reflect new engagements or changes to existing Subprocessors.

7.3 Customer may subscribe to receive email notifications of updates to the Subprocessor List by submitting a request to privacy@janusintl.com. If Customer does not subscribe, the Supplier's update to the publicly available Subprocessor List shall constitute sufficient notice of such changes.

7.4 Customer may object in writing to a new Subprocessor within fifteen (15) days, provided the objection is based on a demonstrable risk of material non-compliance with Applicable Data Protection Laws. Customer acknowledges that objections must not be made unreasonably or in bad faith. Supplier shall not be required to delay the engagement of a proposed Subprocessor where the objection lacks a specific and demonstrable basis under Applicable Data Protection Laws.

7.5 If Customer objects to a Subprocessor, Supplier may, at its sole discretion, assess whether a commercially reasonable alternative exists. If no such alternative is feasible, Customer may, as its sole and exclusive remedy, terminate only the specific services involving the objected Subprocessor, provided that such termination does not impact any unrelated Processing activities or the overall Service Agreement.

8. INTERNATIONAL PROCESSING

8.1 Supplier will only transfer Personal Data originating from the United Kingdom ("**UK**"), European Economic Area ("**EEA**"), Switzerland, or Quebec, Canada to a location outside of the UK, EEA, Switzerland, or Quebec where:

8.1.1 Such transfer is made to Customer or a Customer affiliate at Customer's request or consent (including any Customer group company or personnel), and for the purposes of this Section 8.1, Customer consents to the transfer of Personal Data to the Supplier's Subprocessors and subcontractors appointed from time to time in accordance with this DPA and/or Section 7 of this DPA; and

8.1.2 The transfer is otherwise made in compliance with the SCCs, the UK Addendum, Swiss FADP, Quebec Transfer Clauses, or any other valid and legally recognized cross-border transfer mechanism under Applicable Data Protection Laws.

8.2 Where required by Applicable Data Protection Laws, Supplier shall assist Customer in conducting and documenting any legally required assessments before transferring Personal Data across borders or engaging in Processing activities that necessitate such assessments. Upon request, Supplier shall provide relevant Processing and security information reasonably necessary for conducting these assessments.

8.3 Where Personal Data is transferred from the EEA to a jurisdiction that has not been determined to provide an adequate level of data protection by the European Commission, the SCCs are hereby incorporated by reference, forming an integral part of this DPA, and shall be deemed fully executed and legally binding as of the Agreement Date, without the need for further signatures. The SCCs shall govern such transfers and apply as follows:

8.3.1 Customer acts as the data exporter and Controller, and Supplier acts as the data importer and Processor, as those terms are defined under the SCCs.

8.3.2 If Supplier acts as a Processor, Module 2 (Controller-to-Processor) applies;

8.3.3 If Supplier acts as an independent Controller, Module 1 (Controller-to-Controller) applies;

8.3.4 If Supplier acts as a Subprocessor, Module 3 (Processor-to-Processor) of the Standard Contractual Clauses shall apply;

8.3.5 Clause 7 (Docking Clause) applies;

8.3.6 If Supplier acts as a Processor or Subprocessor, Customer generally authorizes Supplier to engage Subprocessors under Clause 9, option 2 of Module 2;

8.3.7 If Supplier acts as a Controller, Clause 9 shall not apply.

8.3.8 Clause 10 applies, and each Party shall respond directly to Data Subject rights requests except where the Customer, as Controller, instructs Supplier to assist in accordance with Clause 4.5.1 of the DPA;

8.3.9 Parties do not select the Redress mechanism under Clause 11(a);

8.3.10 Pursuant to Clause 13, the competent supervisory authority shall be the supervisory authority of the EU member state where the exporter is established;

8.3.11 Parties choose Option 1 of Clause 17, selecting the laws of Ireland as the governing law; and

8.3.12 Pursuant to Clause 18, any disputes arising from the SCCs shall be subject to the jurisdiction of the courts of Ireland.

8.3.13 For the avoidance of doubt, this Section 8.3 and Appendix 1 Annexes I, II, and III shall constitute Annexes I, II, and III of the SCCs. In the event of any conflict or inconsistency between the SCCs and this DPA, the terms of the SCCs shall prevail.

8.4 Where Personal Data is transferred from the UK to a jurisdiction that has not been determined to provide an adequate level of data protection by the UK government, the UK Addendum is hereby incorporated by reference, forming an integral part of this DPA, and shall be deemed fully executed and legally binding as of the Agreement Date, without the need for further signatures. The UK Addendum shall govern such transfers and apply in the same manner as the SCCs under Section 8.3, except as modified below to align with the UK Addendum's requirements, as follows:

8.4.1 The competent supervisory authority shall be the UK Information Commissioner's Office pursuant to Clause 13;

8.4.2 Parties choose the laws of England and Wales as the governing law under Clause 17;

8.4.3 Any disputes arising under the UK Addendum shall be resolved by the courts of England and Wales, pursuant to Clause 18; and

8.4.4 Parties agree that neither Party shall unilaterally terminate this UK Addendum pursuant to Section 19 of the UK Addendum, except where required by Applicable Laws or regulatory guidance.

8.4.5 The UK Addendum, in the form published by the ICO under s119A(1) Data Protection Act 2018, is incorporated into this DPA as if set forth in full herein and shall apply in conjunction with the SCCs as outlined in Section 8.3. For the avoidance of doubt, this Section 8.4 and Appendix I, Annex I shall serve as Tables 1 and 2 of the UK Addendum; Appendix 1, Annexes I, II, and III shall serve as Table 3; and Section 8.4, Clause 8.4.4 shall serve as Table 4.

8.5 Where Personal Data is transferred from Switzerland to a jurisdiction that has not been determined to provide an adequate level of data protection under the Swiss FADP, the Swiss Addendum are hereby incorporated by reference, forming an integral part of this DPA, and shall be deemed fully executed and legally binding as of the Agreement Date, without the need for further signatures. The Swiss Addendum shall govern such transfers and apply in the same manner as the SCCs under Section 8.3, except as modified to comply with the Swiss FADP, as follows:

8.5.1 The term "Member State" in the SCCs shall be interpreted to include Switzerland, and references to the EU GDPR shall be understood as references to the Swiss FADP;

8.5.2 Where applicable, the SCCs shall be interpreted in conjunction with the FDPIC's guidance on international data transfers under the Swiss FADP;

8.5.3 References to the competent supervisory authority shall mean the Swiss Federal Data Protection and Information Commissioner (FDPIC);

8.5.4 References to "Regulation (EU) 2016/679" or "GDPR" shall be understood as references to the Swiss FADP;

8.5.5 The Swiss Addendum shall apply to Data Subjects in Switzerland, regardless of whether the Processing falls within the territorial scope of the GDPR, consistent with FDPIC guidance on international data transfers;

8.5.6 Clause 17 shall be modified to specify Swiss law as the governing law, as required under the Swiss FADP; and

8.5.7 Clause 18 (Jurisdiction) shall be modified so that disputes shall be resolved in Swiss courts.

8.5.8 For the avoidance of doubt, Section 8.3 as modified by this Section 8.5 and Appendix 1 Annexes I, II, and III shall constitute Annexes I, II, and III of the Swiss Addendum. In the event of any conflict or inconsistency between the Swiss Addendum and this DPA, the terms of the Swiss Addendum shall prevail.

8.6 Where Personal Data is transferred from Quebec to a jurisdiction that has not been determined to provide an adequate level of data protection under Law 25, the Quebec Transfer Clauses are hereby incorporated by reference, forming an integral part of this DPA, and shall be deemed fully executed and legally binding as of the Agreement Date, without the need for further signatures. The Quebec Transfer Clauses shall govern such transfers and apply as follows:

8.6.1 Customer acts as the data exporter and Controller, and Supplier acts as the data importer and Processor, as those terms are defined under the Quebec Transfer Clauses;

8.6.2 Customer provides general authorization for Supplier to engage Subprocessors, in accordance with Section 18.3 of Law 25, Appendix 1, Annex 3; and

8.6.3 The competent supervisory authority shall be the Commission d'accès à l'information du Québec.

8.6.4 For the purposes of Quebec cross-border transfers, this Section 8.6, together with Appendix 1, Annexes I and II constitute the required contractual safeguards under Law 25. The list of authorized Subprocessors, as required under Article 18(3) of Law 25, is provided in Appendix 1, Annex III.

9. GENERAL TERMS

9.1 Liability

Each Party shall be liable solely for damages arising from its breach of this DPA or Applicable Data Protection Laws, subject to the following:

9.1.1 Customer remains solely responsible for the lawfulness, accuracy, and sufficiency of the Personal Data it provides to Supplier, including obtaining any necessary consents or other legal bases for Processing.

9.1.2 Supplier shall not be liable for Processing undertaken in accordance with Customer's Instructions unless Supplier knew or reasonably should have known that such Instructions violated Applicable Data Protection Laws.

9.1.3 Customer shall indemnify and hold harmless Supplier against any third-party claims, fines, or penalties arising from Customer’s failure to comply with its obligations under this DPA or Applicable Data Protection Laws, to the extent permitted by law.

9.1.4 For clarity, this Section 9 does not expand or override any limitations of liability set forth in the Service Agreement, except solely with respect to breaches of this DPA or Applicable Data Protection Laws.

9.2 Conflicts

The Applicable Data Protection Laws shall prevail if there is any conflict with a provision of this DPA. This DPA shall be interpreted to comply with all Applicable Data Protection Laws. In the event of a conflict between this DPA and any other agreement, including the Service Agreement, between the Parties regarding Personal Data Processing, this DPA shall control. All non-conflicting terms of such agreements remain in full force and effect.

9.3 Survival

The obligations of this DPA shall survive the termination or expiration of the Service Agreement for as long as Supplier or any engaged Subprocessor continues to Process Personal Data. Upon cessation of Processing, Supplier shall erase or return Personal Data pursuant to Section 4.4 of this DPA.

9.4 Amendments

Supplier may update this DPA to reflect changes in Applicable Data Protection Laws, regulatory guidance, or best practices. Supplier shall notify Customer of material updates through the contact methods indicated in the Service Agreement, or by posting such updates online at https://wwwjanusintl.com/resources/forms. Updates shall become binding thirty (30) days after notice or posting unless Customer provides a written objection demonstrating a material adverse impact. If an objection is raised, the Parties shall negotiate in good faith to reach a mutually acceptable resolution.

9.5 Compensation

Unless otherwise expressly stated herein, the Supplier's right for compensation is exclusively regulated in the Service Agreement.

9.6 Non-Assignment

Neither Party may assign or transfer any rights or obligations under this DPA, in whole or in part, without the prior written consent of the other Party. Any attempted assignment in violation of this Section 9.6 shall be null and void.

9.7 Third-Party Rights

This DPA benefits only the Parties and their permitted successors and assigns. No third party shall have any rights, remedies, or claims under this DPA, whether by contract, statute, or otherwise.

9.8 Governing Law

This DPA shall be governed by and construed in accordance with the governing law specified in the Service Agreement, except where Applicable Data Protection Laws require otherwise. Where such law mandates a specific governing jurisdiction, that jurisdiction shall apply to the extent required.

9.9 **Integration**

This DPA, together with the Service Agreement and any referenced appendices, annexes, and schedules, constitute the entire agreement between the Parties regarding Personal Data Processing and supersedes all prior agreements, written or oral, concerning the same. For clarity, all other terms of the Service Agreement remain unchanged.

[INTENTIONALLY LEFT BLANK]

APPENDIX 1

This Appendix, including its Annexes, forms part of the DPA and outlines the scope, nature, and purpose of Personal Data Processing, the categories of Data Subjects, and the security measures in place. It is designed to comply with cross-border data transfer requirements under Applicable Data Protection Laws, including the GDPR, UK GDPR, Swiss FADP, and Law 25.

This Appendix includes:

- **Annex 1**: Parties and Data Transfer Details
- **Annex 2**: Security Measures
- **Annex 3**: Authorized Subprocessors

In case of conflict, this Appendix prevails for data processing and transfer matters.

ANNEX I

A. LIST OF THE PARTIES

Data exporter(s):

Name: CUSTOMER

Address: As specified in the Service Agreement.

Position and contact details: As specified in the Service Agreement.

Activities relevant to the data transferred under the SCCs, UK SCCs, Swiss Addendum, and the Quebec Transfer Clauses: As described in the Service Agreement.

Signature and date: Executed as of the Agreement Date

Role (controller/processor): Controller

Data importer(s):

Name: JANUS INTERNATIONAL GROUP, LLC

Address: 135 Janus International Boulevard, Temple, GA 30179, United States

Position and contact details: Privacy Officer, +1 770.562.6055; privacy@janusintl.com

Activities relevant to the data transferred under the SCCs, UK SCCs, Swiss Addendum, and the Quebec Transfer Clauses: As described in the Service Agreement

Signature and date: Executed as of the Agreement Date

Role (controller/processor): Processor and Controller

B. DESCRIPTION OF THE TRANSFER

Supplier acting as a Processor	
Categories of Data Subjects	The following categories of Data Subjects' Personal Data will be Processed under this DPA: • Customers; • Customer’s personnel (including Customer’s personnel who are End

	Users); • Third-party End Users; and • Tenants and other End Users (including users authorised by tenants).
Categories of Personal Data	The following categories of Personal Data will be Processed: • Customer first and last name; • Customer business and personal email; • Customer Unit Number(s); • Customer activity data (such as opening and closing of access points); • Customer personnel contact details; • End User first and last name; • End User contact details; • Tenant Unit Number(s); • End User access credentials; • End User location (when in close proximity of a Unit and the Services are activated); and • End User activity data (such as opening and closing of access points).
Categories of Special Category Personal Data	• Supplier, when acting as a Controller, does not intend to Process any categories of Special Personal Data (as defined by the GDPR).
Processing Operations	The Personal Data will be subject to the following basic processing activities: • Collection; • Storage; • Retrieval; • Disclosure by transmission; • Combination (limited to operational functions in accordance with Customer's Instructions (e.g., security, access control, troubleshooting); and • Erasure.
Purpose(s) of the Processing and Legal Bases	The Personal Data will be Processed for the following purpose(s): • **Contractual necessity: to provide the Services** under the Service Agreement, maintain operation, maintenance, and performance of the agreed-upon services; maintain, improve, and enhance the quality, security, and efficiency of the Services provided; facilitate user authentication and access control for End Users; • **Legal obligation:** comply with legal and regulatory obligations applicable to Supplier; **Legitimate interest:** maintaining the security, availability, and functionality of the Services (including fraud prevention and operational continuity) while providing safeguards to protect Data Subjects' rights and freedoms; and **Consent:** where required by law, explicit consent obtained before processing certain categories of personal data (e.g., geolocation data, marketing purposes).
Retention of Personal Data	Supplier shall retain Personal Data solely for Processing purposes under this DPA, subject to applicable legal retention requirements. Where feasible, Supplier shall implement data minimization principles in accordance with industry standards and legal obligations. Backup and archival data shall be retained as necessary for business continuity, disaster recovery, and compliance with legally mandated retention obligations.

Supplier acting as a Controller	
Categories of Data Subjects	The following categories of Data Subjects' Personal Data will be Processed under this DPA: • Customers and Customers' personnel; and • Tenants and other End Users (including users authorised by tenants)
Categories of Personal Data	The following categories of Personal Data will be Processed: • Customer activity data (such as opening and closing of access points, use of the Services for troubleshooting, monitoring, and enhancements); • End User activity data (such as opening and closing of access points, use of the Services for troubleshooting, monitoring, and enhancements); • End User location data (when in close proximity to a Unit and the Services are activated).
Categories of Special Category Personal Data	Supplier, when acting as a Controller, does not intend to Process any categories of Special Personal Data (as defined by the GDPR).
Processing Operations	The Personal Data will be Processed in the following ways: • Collection; • Storage; • Retrieval; • Combination (limited to internal research for technological development); and • Erasure.
Purpose(s) of the Processing and Legal Bases	The Personal Data will be Processed for the following purpose(s): • **Legitimate interest**: supports product development and improvement, (e.g., usage patterns and behavioral data to improve features and enhance service offerings; analytics (e.g., product performance assessment and maintaining internal analytics reports); • **Legal obligations:** legal and regulatory compliance. • **Consent:** marketing & communications, including opt-in mechanisms where explicit consent is required by law.
Retention of Personal Data	The Supplier will retain Personal Data as a Controller in accordance with documented retention policies that align with minimization principles pursuant to Applicable Data Protection Laws.

C. DESCRIPTION OF THE TRANSFER CONTINUED

Categories of data subjects whose personal data is transferred

Affected individuals will include those categories of Data Subject specified in Annex 1, Section B.

Categories of personal data transferred

The categories of personal data affected shall include those types of personal data specified in Annex 1, Section B.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved

Supplier does not intend to Process or transfer any special categories of Personal Data (as defined under GDPR Article 9) or sensitive Personal Data (as defined under Applicable Data Protection Laws) (collectively, "**Sensitive Personal Data**") under the Service Agreement.
If such data is inadvertently processed or transferred, Supplier shall:

- Implement appropriate technical and organizational measures ("**TOMs**") to protect the data, including encryption, access controls, and data minimization.
- Verify that Processing is limited to what is necessary for the provision of the Services and, where applicable, to provide the Services (e.g., geolocation data for security purposes).
- Notify Customer if Supplier becomes aware that it has received Sensitive Personal Data not covered under this DPA and take commercially reasonable steps to erase such data, unless retention is required by Applicable Data Protection Laws.
- Adhere to any additional safeguards required under Applicable Data Protection Laws, including obtaining explicit consent where legally required.

The frequency of the transfer

Transfers are expected to occur continuously, with the possibility of pre-scheduled batch transmissions.

Nature of the processing

The types of processing activity conducted shall include the processing activities specified in Annex 1, Section B.

Purpose(s) of the data transfer and further processing

The purposes of transfers shall include the purposes specified in Annex 1, Section B.

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

1. **When Supplier Acts as a Processor:**
   - Personal Data shall be retained only for the duration necessary to fulfill the obligations under the Service Agreement, including any applicable retention periods required by Customer's Instructions or Applicable Laws;
   - Upon termination or expiration of the Service Agreement, Supplier shall either securely erase or return the Personal Data in accordance with Section 4.4.4 of this DPA, unless prohibited by Applicable Laws.
2. **When Supplier Acts as a Controller:**
   - Supplier shall retain Personal Data only for as long as necessary to fulfill the purposes for which it was collected, in accordance with its documented retention policies and legal obligations.
   - Retention periods shall be determined based on legitimate business needs, legal and

- regulatory requirements, industry best practices, and applicable contractual obligations.
- Where required by Applicable Laws, Supplier shall implement appropriate data minimization and secure disposal procedures.

3. **Personal Data Stored in Backup or Archival Systems:**
   - Supplier retains Personal Data only as required for its obligations under the Service Agreement or Applicable Laws. Backup and archival data shall be erased per Supplier's retention policy.
4. **Criteria for Determining Retention Periods:**
   - The nature, purpose, and necessity of the Processing.
   - Legal, regulatory, and contractual requirements, including any statutory retention obligations.
   - The existence of ongoing legal claims, audits, or compliance obligations that necessitate continued retention.

If Personal Data is no longer necessary for the purposes for which it was collected and there is no legal obligation to retain it, Supplier shall securely erase, anonymize, de-identify, or aggregate, as appropriate.

D. COMPETENT SUPERVISORY AUTHORITY

The following supervisory authorities shall apply for cross-border transfers of Personal Data, in accordance with Applicable Data Protection Laws:

1. to Clause 13, the competent supervisory authority shall be the supervisory authority of the EU member state where the exporter is established
2. For UK GDPR transfers, the UK Information Commissioner’s Office (ICO) shall be the competent authority.
3. For Swiss FADP transfers, the Swiss Federal Data Protection and Information Commissioner (FDPIC) shall be the competent authority.
4. For Law 25 transfers, the Commission d’accès à l’information du Québec (CAI) shall be the competent authority.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES

The Supplier shall implement and maintain appropriate technical and organizational security measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. These measures are designed to provide a level of security appropriate to the risk and are implemented in accordance with Applicable Data Protection Laws. The measures include, but are not limited to, the following:

1. **Organizational Controls**
    - Implementation of a formal, documented information security program that governs the protection of Personal Data and is subject to regular review and risk-based updates.
    - Assignment of roles and responsibilities for information security, including the designation of a security officer and privacy lead.
    - Regular employee security awareness training, including phishing prevention, secure data handling, and role-specific data protection protocols.
    - Formal onboarding and offboarding procedures for personnel with access to Personal Data.
2. **Access Controls and Confidentiality**
    - Role-Based Access Control mechanisms for access to systems and Personal Data is granted based on the principle of least privilege.
    - Multi-Factor Authentication for all user accounts.
    - Logical separation of environments (e.g., production, development, and testing) to prevent unauthorized data exposure.
    - User authentication, access logging, and audit trails for all administrative access.
    - Confidentiality agreements for all employees and contractors with access to Personal Data.
    - Access to Personal Data is limited to individuals with a business need.
3. **Network and System Security**
    - Segregated Virtual Private Cloud environments with firewall configurations to isolate and protect systems.
    - Endpoint Detection and Response, intrusion detection and prevention systems, and antivirus/anti-malware software.
    - Encryption of Personal Data in transit using TLS 1.2 or higher and at rest using AES-256 or an equivalent industry-standard algorithm.
    - Secure encryption key management practices, including rotation, storage in secure key vaults, and access limitation.
    - Use of Secure Software Development Lifecycle practices, including static code analysis, vulnerability scanning, and peer code review.
4. **Monitoring and Incident Response**
    - Continuous monitoring of systems and networks, including automated logging and real-time alerting for security events.
    - Retention of audit logs in a secure manner for a period appropriate to the risk and legal obligations.
    - Documented incident response plan that defines roles, responsibilities, escalation procedures, and Customer notification obligations as expressly set forth in the Service Agreement.
    - Supplier maintains procedures designed to investigate security incidents involving Personal Data and to notify Customers of a confirmed Personal Data Breach solely to the extent required by Applicable Law or the Service Agreement.
5. **Data Integrity and Availability**
    - Regular backup of critical systems and Personal Data supporting the Services, with

- encrypted offsite storage where appropriate, in a manner commensurate with the criticality of the Services provided under the Service Agreement.
- Implementation of a disaster recovery and business continuity plan applicable to the systems supporting the Services, which is reviewed and tested periodically in accordance with the risk and criticality of those Services.
- Patch management policies for timely updates and remediation of known vulnerabilities in operating systems, applications, and infrastructure.
- Use of high availability infrastructure and redundancy strategies to reduce the risk of data loss or downtime.

6. **Subprocessor and Vendor Management**
    - Subprocessors are contractually bound to implement equivalent security measures and are subject to risk-based due diligence prior to engagement.
    - Ongoing oversight of Subprocessors, including periodic audits or certifications and review of security performance.
    - Supplier maintains a list of current Subprocessors available to the Customer via publication on Supplier's site or other reasonable means in accordance with the DPA.
7. **Data Minimization and Privacy Enhancing Techniques**
    - Personal Data is collected and retained as necessary for the purposes defined in the Service Agreement and by Applicable Data Protection Laws.
    - Where feasible and appropriate, Supplier implements techniques, such as data masking, to limit direct identifiability of data subjects.
8. **Security Certifications and Audits**
    - Upon written request no more than once annually, Supplier shall make available to Customer a summary of its most recent third-party audit reports or certifications relevant to the Services.

ANNEX III - LIST OF SUB-PROCESSORS

The Customer has generally authorised the use of the Subprocessors listed at www.janusintl.com/subprocessors.

Commented [CW1]: Link to page. p

APPENDIX 2

LIST OF AFFILIATES

Janus International Canada, Ltd.

- Registered Office: Skylaw, 22 St. Clair Avenue East, Suite 200, Toronto, Ontario M4T 2S3, Canada
- Principal Place of Business: 135 Janus International Blvd Temple, GA 30179

Janus International Europe Ltd (UK)

- Registered Office: 102b The Green, Twickenham, Middlesex, United Kingdom, TW2 5AG
- Principal Place of Business: Same.

Noke, Inc.

- Registered Office: 251 Little Falls Drive, Wilmington, DE 19808, United States
- Principal Place of Business: 2000 W. Ashton Blvd. Suite 375 Lehi, UT 84043