DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms part of the Master Sales, Service, and License Agreement or other written agreement that incorporates this DPA ("**Service Agreement**") between **Customer** and **Janus International Group LLC**, 135 Janus International Boulevard, Temple, Georgia 30179, United States, acting for itself and, to the extent authorized, the Affiliates identified in Appendix 2 that provide the Services ("**Supplier**"). Each is a "**Party**" and together they are the "**Parties**." This DPA becomes binding when the Parties enter into the Service Agreement incorporating it ("**Agreement Date**"), without a separate signature. An Affiliate's listing does not, by itself, make it a separate contracting party or establish a cross-border transfer safeguard.

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 acts as a Processor where Customer is a Controller, and as a Subprocessor where Customer is a Processor acting on a Controller's behalf. Supplier acts as an independent Controller only for the Processing described in Section 4 and Appendix 1 that it lawfully determines for its own purposes. The Parties' roles depend on the relevant Processing and Applicable Data Protection Laws, not solely on contractual labels.

D Any conflict between the Service Agreement and this DPA shall be resolved in accordance with Section 8.2 (Conflicts).

1. 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, Regulation (EU) 2016/679 (the General Data Protection Regulation) ("**GDPR**"); the UK General Data Protection Regulation ("**UK GDPR**"), as defined in section 3(10) of, and supplemented 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; Quebec's Act respecting the protection of personal information in the private sector, CQLR c. P-39.1 (the "**Quebec Private Sector Act**"), as amended by the 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

Confidential

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 a Party or other person or entity that, alone or jointly with others, 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 otherwise 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 a person or entity that Processes Personal Data on behalf of a Controller, including Supplier when it Processes Personal Data on behalf of Customer or another Processor, and including roles equivalent to a Processor, Subprocessor, Service Provider, or Contractor 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 provisions in Section 7.6 and Appendix 1 addressing requirements applicable to the relevant Processing under Sections 17 and 18.3 of the Quebec Private Sector Act. The term does not imply regulatory approval or automatically incorporate future model clauses.

Confidential

"**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 a third party, including an Affiliate, engaged by a Processor to Process Personal Data on a Controller's behalf. Supplier acts as a Subprocessor where Customer is a Processor. Supplier personnel and individuals acting under Supplier's direct authority are not separate Subprocessors solely by reason of that access; independent contractors performing delegated Processing are assessed according to their actual functions and Applicable Data Protection Laws. Supplier's engaged Subprocessors are identified in Appendix 1, Annex III.

"**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.

2. CUSTOMER OBLIGATIONS

Customer is responsible for the lawfulness of its collection, use, disclosure, and Instructions concerning Personal Data, including required notices, consents or other authorization, and the accuracy and adequacy of data it supplies. Where Customer acts as a Processor, Customer represents that the relevant Controller has authorized the Services, Supplier's appointment, further Subprocessors, and the Instructions and transfers contemplated by this DPA. Customer shall communicate relevant Controller instructions and required notices through Customer and obtain any additional upstream authorization required by Applicable Data Protection Laws. Supplier may rely on Customer's authority without independently verifying it, except where legally required. Customer shall not provide sensitive data outside the agreed scope without Supplier's prior written agreement. Nothing in this Section relieves Supplier of obligations applicable to its own Processing.

3. SUPPLIER OBLIGATIONS AS A PROCESSOR

3.1 Compliance with Instructions

Supplier shall Process Personal Data on Customer's behalf only on documented Instructions, including regarding transfers. This DPA, the Service Agreement, and Customer's use and configuration of the Services constitute such Instructions. Additional Instructions outside the agreed scope require agreement on feasibility, timing, and any applicable fees; pending agreement, Supplier shall continue lawful Processing under existing Instructions and shall not undertake the disputed additional Processing. Mandatory obligations under Applicable Data Protection Laws remain unaffected.

Confidential

3.2 **Legal Obligations**

Supplier may Process Personal Data without Instructions only to the extent permitted or required by Applicable Data Protection Laws. Where Article 28(3)(a) of the GDPR or UK GDPR applies, the exception is limited to the law specified therein, and Supplier shall inform Customer of the legal requirement before Processing unless that law prohibits notice on important grounds of public interest. Public-authority requests and third-country disclosure requirements remain subject to applicable transfer restrictions and, where applicable, the SCCs. Supplier need not implement unlawful Instructions and may suspend the affected Processing while the Parties seek a lawful resolution.

3.3 **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.

3.4 **Supplier Commitments as a Processor**

In acting as Processor, Supplier shall:

3.4.1 Maintain Processing records to the extent required by Applicable Data Protection Laws and make available information necessary to demonstrate compliance with applicable Processor obligations, subject to Section 5.3 and reasonable confidentiality and security protections that do not prevent legally required disclosure;

3.4.2 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;

3.4.3 To the extent required by Applicable Data Protection Laws (including Clause 15 of the SCCs, where applicable), notify Customer of any legally binding request by a public authority for access to or disclosure of Personal Data Processed on Customer's behalf, unless such notification is prohibited by Applicable Laws;

3.4.4 Following the end of Services involving Processing on Customer's behalf, return or securely delete that Personal Data at Customer's election communicated in writing within thirty (30) days; absent an election, Customer instructs Supplier to securely delete it. Supplier shall delete remaining copies after return, except to the extent storage is required by a law permitting retention under Applicable Data Protection Laws. Return may be in Supplier's standard export format. This paragraph does not govern Personal Data lawfully retained by Supplier as an independent Controller under Section 4 and Appendix 1.

3.4.5 To the extent permitted by Applicable Data Protection Laws, residual copies in non-production backups shall be isolated from ordinary use, protected under this DPA, and deleted through Supplier's ordinary secure overwrite or deletion cycle. Restoration shall not authorize renewed use beyond disaster recovery or legally required purposes, and applicable deletion Instructions shall be reapplied. This paragraph does not authorize retention prohibited by Applicable Data Protection Laws.

Confidential

3.5 **Assistance with Compliance**

Only to the extent required by Applicable Data Protection Laws, taking into account the nature of Processing and information available to Supplier, Supplier shall assist Customer as follows:

3.5.1 Notify Customer of Data Subject requests concerning Processing on Customer's behalf and assist, through appropriate technical and organizational measures insofar as possible, with Customer's legally required response. Supplier may direct the requester to Customer and shall not otherwise respond substantively except on Instructions or as legally required;

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

3.5.3 Supplier may satisfy assistance requests through available Service functionality, documentation, and existing reports where sufficient. Supplier may charge reasonable fees for additional assistance to the extent permitted by Applicable Data Protection Laws, except for assistance necessitated by Supplier's breach of this DPA. Fees shall not condition or delay performance of a non-waivable legal obligation.

3.6 **CCPA Obligations**

3.6.1 This Section applies only to Personal Data subject to the CCPA and Processed by Supplier as a Service Provider or Contractor (each as defined in the CCPA), including where Customer is itself a Service Provider or Contractor authorized to engage Supplier. Customer discloses such data only for the limited, specified business purposes of administering storage-facility access, authenticating users, managing digital credentials, recording access events, hosting and maintaining the Services, troubleshooting, support, and security, as applicable to the Services purchased and detailed in Appendix 1. The Parties intend this disclosure not to constitute Sale or Sharing. Any consideration is for the Services, not the Personal Data. Supplier certifies that it understands and will comply with the applicable restrictions in this Section.

3.6.2 Supplier Obligations as a Service Provider or Contractor

3.6.2.1 When acting as a Service Provider or Contractor, Supplier shall:

(a) Not retain, use, or disclose such Personal Data for purposes other than the specified business purposes, including any other commercial purpose, or outside the direct business relationship, except as expressly permitted by the CCPA and its regulations. Permitted internal service improvement and security uses remain subject to those restrictions. Section 4 does not expand the uses permitted for Personal Data received in this capacity;

(b) Not Sell or Share Personal Data;

Confidential

(c) 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;

(d) Allow Customer to take reasonable and appropriate steps to verify that Supplier uses such Personal Data consistently with Customer's CCPA obligations and, upon notice, to stop and remediate unauthorized use, subject to Section 5.3 only to the extent its procedures do not restrict these legally required rights;

(e) Notify Customer if Supplier determines that it can no longer meet its applicable CCPA obligations and cooperate with reasonable and appropriate steps to stop and remediate unauthorized use as required by the CCPA;

(f) Comply with applicable CCPA obligations and provide the level of privacy protection required by the CCPA for Personal Data Processed in the Service Provider or Contractor capacity described in this Section; and

(g) Engage any subcontractor to Process such Personal Data pursuant to a written contract imposing obligations no less protective than those in this Section 3.6.

3.6.2.2 Customer shall inform Supplier of any consumer request under the CCPA with which Supplier must comply and provide the information necessary for Supplier to comply.

4. SUPPLIER OBLIGATIONS AS A CONTROLLER

4.1 Each Party is independently responsible for compliance with Applicable Data Protection Laws for Processing it undertakes as a Controller, including lawful bases, required notices and consents, Data Subject rights, retention, and legally required breach reporting. Supplier does not assume Customer's Controller obligations.

4.2 Supplier may act as an independent Controller for business-relationship administration and communications, legal compliance and claims, and lawful security, product-development, and analytics purposes described in Appendix 1, Annex I. This may include Usage Data, as defined in the Service Agreement, but only where Supplier lawfully determines the relevant purposes and means. Credentialing, access records, and other data Processed to deliver Services on Customer's behalf remain subject to the Processor provisions for that Processing.

4.3 To the extent permitted by Applicable Data Protection Laws and applicable Instructions, Supplier may de-identify, pseudonymize, aggregate, derive information from, or, where technically feasible, anonymize Personal Data. Any resulting data that remains Personal Data continues to be subject to this DPA. Supplier shall apply measures required by Applicable Data Protection Laws to data it treats as no longer constituting Personal Data, including any required commitments not to re-identify, public commitments, and recipient restrictions. No provision

Confidential

authorizes otherwise prohibited secondary use or overrides Customer's applicable return or deletion election.

4.4 For purposes of this DPA, "Derivative Data" and "Usage Data" have the meanings given in the Service Agreement and include only information that satisfies the applicable requirements in those definitions. As between the Parties, ownership and permitted use of Derivative Data and Usage Data are governed by the Service Agreement, subject to this DPA and Applicable Data Protection Laws. Supplier may use or disclose Derivative Data and Usage Data as permitted by the Service Agreement and this DPA.

5. SECURITY MEASURES

5.1 Obligation to Implement Technical and Organizational Measures to Protect Personal Data

5.1.1 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 Appendix 1, Annex II, which applies to all Processing under this DPA.

5.1.2 Supplier's assistance concerning security assessments and regulatory consultations is governed by Section 3.5. Section 5.3 governs related compliance verification. Neither provision requires disclosure of other customers' data, privileged material, or information that would compromise security, except to the extent disclosure is legally required and subject to available protective measures.

5.2 **Personal Data Breach**

5.2.1 For Personal Data Processed on Customer's behalf, Supplier shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting that data, or within any shorter period required by Applicable Data Protection Laws, and provide additional relevant information as it becomes available. For its independent Controller Processing, Supplier is responsible for notices required of it by Applicable Data Protection Laws. Unsuccessful attempts that do not compromise Personal Data do not constitute a Personal Data Breach; Section 7.6.5 remains unaffected.

5.2.2 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; (ii) the likely consequences of the breach, if known; (iii) the measures taken or proposed to be taken by Supplier to address the breach and mitigate its possible adverse effects; and (iv) the name and contact details of Supplier's point of contact for further information.

5.2.3 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.

5.3 **Audit Rights and Compliance Verification**

Confidential

5.3.1 For Processing on Customer's behalf, Supplier shall allow and contribute to audits, including inspections, to the extent required by Applicable Data Protection Laws. Subject to Section 5.3.2, routine audits are limited to one per calendar year on thirty (30) days' written notice, during normal business hours, by Customer or an independent auditor reasonably acceptable to Supplier and bound by confidentiality obligations. These limits do not apply where a shorter notice period or additional audit is legally required, required by a competent authority, or reasonably necessary to investigate reasonable indications of non-compliance with this DPA or a Personal Data Breach affecting Customer's data. Audits shall be proportionate and avoid unnecessary disruption or access to unrelated data.

5.3.2 Where Supplier maintains industry-recognized security certifications or third-party audit reports (e.g., SOC 2), Supplier will make available the most recent such reports upon request, and Customer agrees to rely on such reports in the first instance. A direct audit under Section 5.3.1 shall be permitted only where (i) such reports are not available or do not reasonably address Customer's specific compliance concerns; (ii) there are indications of non-compliance with this DPA; (iii) a Personal Data Breach affecting Customer's Personal Data has occurred; or (iv) an audit is required by Applicable Data Protection Laws or a competent supervisory authority.

5.3.3 Customer shall bear its audit costs and reasonable fees for Supplier's assistance to the extent permitted by Applicable Data Protection Laws, except additional assistance necessitated by Supplier's breach. Supplier shall address identified non-compliance with its obligations within a timeframe appropriate to the nature and risk of the issue and applicable legal requirements. Reasonable confidentiality, security, and access protocols apply but shall not prevent exercise of mandatory audit rights. This Section does not require Supplier to reimburse Customer's audit costs except as required by law or the Service Agreement.

6. USE OF SUBPROCESSORS

6.1 Customer grants general written authorization for Supplier to engage Subprocessors for Processing on Customer's behalf. Supplier shall impose by written contract the data-protection obligations no less protective than those applicable to Supplier under this DPA for the delegated Processing, including appropriate security and confidentiality obligations. Supplier remains responsible for each engaged Subprocessor's performance of those obligations to the extent required by Applicable Data Protection Laws and applicable SCCs, subject to Section 8.1 to the extent legally permitted.

6.2 Supplier maintains the authoritative list of authorized Subprocessors at www.janusintl.com/subprocessors ("**Subprocessor List**"), incorporated by reference into Appendix 1, Annex III. Supplier may provide the list directly if the website is unavailable. The version applicable as of the Agreement Date identifies the initially authorized Subprocessors; subsequent additions and replacements are governed by Sections 6.3 through 6.5.

6.3 Where Applicable Data Protection Laws or applicable SCCs require advance notice and an opportunity to object, Supplier shall specifically notify Customer in writing of an intended Subprocessor addition or replacement at least fifteen (15) days before the new Subprocessor begins the relevant Processing, using Customer's designated privacy contact or the contact under the Service Agreement. Supplier shall provide information reasonably necessary to

Confidential

assess the proposed Processing. Customer shall keep its contact details current. Otherwise, updating the Subprocessor List constitutes notice under this DPA. Emergency engagement on shorter notice is permitted only where legally permissible or pursuant to valid prior specific authorization where required; an emergency does not override mandatory notice or authorization requirements.

6.4 Customer may object in writing within fifteen (15) days after notice, on reasonable, specific data-protection grounds concerning the proposed Subprocessor's Processing. If Customer does not timely object, the proposed engagement is authorized. Supplier need not accept objections unrelated to data protection. A timely, reasonable objection shall be addressed under Section 6.5 before the proposed Subprocessor Processes the affected data where required by Applicable Data Protection Laws or applicable SCCs.

6.5 The Parties shall seek a commercially reasonable resolution to a timely, reasonable objection. Supplier may avoid use of the proposed Subprocessor for the affected data, offer an available alternative, or discontinue the affected portion of the Services. Supplier need not redesign the Services or incur disproportionate expense. If no resolution is available, either Party may terminate only the affected Services on written notice before the objected Processing begins where legally required. This is Customer's sole contractual remedy for an otherwise compliant proposed engagement, without limiting mandatory rights under Applicable Data Protection Laws or applicable transfer clauses. Treatment of fees remains governed by the Service Agreement.

7. INTERNATIONAL PROCESSING

7.1 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:

7.1.1 Such transfer is made (a) to Customer or a Customer Affiliate (including any Customer group company or personnel) at Customer's request or with Customer's consent, or (b) to Supplier's Affiliates, Subprocessors, or subcontractors engaged from time to time in accordance with Section 6 of this DPA, to which Customer hereby consents; and

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

7.2 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.

7.3 Where a transfer from Customer to Supplier requires safeguards under Chapter V of the GDPR and is not covered by an applicable adequacy decision or another valid mechanism, the SCCs are incorporated by reference and binding without separate signature as of the Agreement Date. Where Supplier's Processing of the transferred Personal Data is directly subject to the GDPR pursuant to Article 3, Supplier shall comply with the GDPR directly with respect to that Processing, and the SCCs apply as a contractual safeguard for the transfer pending the European

Confidential

Commission's adoption of standard contractual clauses for such importers; upon adoption, the Parties shall implement those clauses for the relevant transfers in accordance with Section 8.4. Nothing in the SCCs limits Supplier's direct obligations under the GDPR. The SCCs apply only to the relevant transfer and Processing, as follows:

7.3.1 Customer acts as the data exporter and Supplier acts as the data importer for all transfers under the SCCs. Customer acts as Controller, or as Processor where Supplier acts as a Subprocessor, and Supplier acts as Processor, Subprocessor, or independent Controller, as set out in Sections 7.3.2 through 7.3.4 and Appendix 1, Annex I, as those terms are defined under the SCCs.

7.3.2 Module 2 (Controller-to-Processor) applies where Customer acts as Controller and Supplier acts as Processor for the relevant transfer;

7.3.3 Module 1 applies where Customer and Supplier each act as independent Controllers. Module 1 is not selected merely because Supplier is a Controller where Customer acts as a Processor. Any Processor-to-Controller transfer must be separately assessed for lawful upstream authority and an appropriate transfer mechanism; Module 4 applies only if its factual and legal requirements are met and the Parties document its application and complete the necessary selections before the transfer.

7.3.4 If Supplier acts as a Subprocessor, Module 3 (Processor-to-Processor) of the SCCs shall apply;

7.3.5 Clause 7 (Docking Clause) applies;

7.3.6 For Modules 2 and 3, Clause 9(a), Option 2 (general written authorization) applies. The prior-notice period is fifteen (15) days, and notice, objections, and resolution are governed by Sections 6.3 through 6.5, without derogating from the SCCs;

7.3.7 If Supplier acts as a Controller, Clause 9 shall not apply;

7.3.8 Clause 10 applies. Where Supplier acts as a Processor or Subprocessor, Supplier shall handle Data Subject rights requests in accordance with Section 3.5.1 of this DPA; where Supplier acts as an independent Controller, each Party shall respond directly to Data Subject rights requests relating to its own Processing;

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

7.3.10 Pursuant to Clause 13, the competent supervisory authority shall be determined in accordance with Clause 13(a) of the SCCs based on the data exporter's establishment or, where applicable, its representative under Article 27 of the GDPR, or, where the data exporter has no such establishment or representative, the supervisory authority of the Member State in which the relevant Data Subjects are located;

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

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

Confidential

7.3.13 For the avoidance of doubt, this Section 7.3 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.

7.4 For a restricted transfer from Customer to Supplier subject to the UK GDPR that requires contractual safeguards and is not covered by an applicable adequacy regulation or another valid mechanism, the UK Addendum is incorporated by reference and binding without separate signature as of the Agreement Date. Where Supplier's Processing is directly subject to the UK GDPR pursuant to its Article 3, Supplier shall comply with the UK GDPR directly, and nothing in the UK Addendum limits those obligations. The SCCs identified in Section 7.3 apply as amended by the UK Addendum's Mandatory Clauses, with the following selections:

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

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

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

7.4.4 For Table 4, both Importer and Exporter may end the UK Addendum in the circumstances and subject to the conditions set out in its Section 19. No selection modifies the Mandatory Clauses or authorizes continued restricted transfers without valid safeguards.

7.4.5 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 7.3. For the avoidance of doubt, Sections 7.3 and 7.4 and Appendix 1, 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 7.4.4 shall serve as Table 4.

7.5 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, and the transfer is not covered by another valid mechanism under the Swiss FADP, the Swiss 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 Swiss Addendum shall govern such transfers and apply in the same manner as the SCCs under Section 7.3, except as modified to comply with the Swiss FADP, as follows:

7.5.1 The term "Member State" in the SCCs shall be interpreted to include Switzerland, so that Data Subjects in Switzerland may exercise their rights in their place of habitual residence in accordance with Clause 18(c) of the SCCs;

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

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

Confidential

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

7.5.5 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;

7.5.6 Clause 17 shall be modified to specify Swiss law as the governing law; and

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

7.5.8 For the avoidance of doubt, Section 7.3 as modified by this Section 7.5 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.

7.6 This Section applies only to the extent the relevant Processing or communication outside Quebec is subject to Sections 17 or 18.3 of the Quebec Private Sector Act. Customer is responsible for its required privacy impact assessment and decision to communicate Personal Data. On request, Supplier shall provide reasonably available information about its relevant Processing and safeguards to support that assessment, subject to Section 3.5. The following provisions apply:

7.6.1 Customer acts as the data exporter and Supplier acts as the data importer. Supplier acts as Processor when Processing Personal Data on behalf of Customer, and as an independent Controller with respect to Usage Data and the other limited purposes set forth in Section 4 and Appendix 1, in each case as such roles are understood under the Quebec Private Sector Act;

7.6.2 Customer provides general authorization for Supplier to engage the Subprocessors identified in the Subprocessor List incorporated into Appendix 1, Annex III, subject to Section 6 and the requirements applicable to the delegated Processing under the Quebec Private Sector Act; and

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

7.6.4 This Section and Appendix 1 record the Parties' contractual safeguards for the relevant Processing. Customer shall assess whether additional safeguards are required by its legally required assessment and agree any necessary additional terms with Supplier before the affected communication. Neither execution of this DPA nor use of the label "Quebec Transfer Clauses" establishes, by itself, that a particular communication satisfies applicable legal requirements.

7.6.5 Where Section 18.3 of the Quebec Private Sector Act applies to Supplier's Processing on Customer's behalf, Supplier shall take the measures required to protect confidentiality, use the information only to perform the mandate or contract, not retain it after that mandate or contract expires, notify Customer's person in charge of personal information protection without delay of any violation or attempted violation of confidentiality, and allow that person to verify compliance. Sections 3.4.4, 3.4.5, and 5.3 apply only insofar as consistent with these

Confidential

requirements and do not create a retention exception or restriction on verification prohibited by that Act.

7.7 Onward Transfers. Customer is the data exporter for all transfers of Personal Data to Supplier under this Section 7. Supplier may make onward transfers of Personal Data to its Affiliates and Subprocessors only in compliance with Clause 8.7 (Module 1) or Clause 8.8 (Modules 2 and 3) of the SCCs, as applicable, and Applicable Data Protection Laws, including by means of intra-group data transfer agreements incorporating the SCCs or another valid transfer mechanism. Data that has been de-identified, pseudonymized, or aggregated in accordance with Section 4.3 remains subject to this Section 7 unless and to the extent it no longer constitutes Personal Data under Applicable Data Protection Laws.

8. GENERAL TERMS

8.1 Liability

As between the Parties, liability arising out of or relating to this DPA is allocated under the Service Agreement and this Section, subject to mandatory Applicable Data Protection Laws and applicable transfer clauses. Nothing in this Section creates an independent remedy, indemnity, or category of recoverable damages except as expressly stated below.

8.1.1 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.

8.1.2 To the extent permitted by Applicable Data Protection Laws, Supplier is not responsible for harm attributable to Customer's unlawful Instructions, unauthorized disclosures, or failure to meet Customer's own obligations. This does not excuse Supplier's breach of its applicable Processor duties, including its duty to notify Customer of an Instruction it considers unlawful, or liability that cannot lawfully be excluded.

8.1.3 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.

8.1.4 To the fullest extent permitted by law, all liability arising out of or relating to this DPA, including its indemnity obligations, is subject to the exclusions, limitations, and aggregate liability caps in the Service Agreement. Claims under this DPA and the Service Agreement count toward the same applicable aggregate cap and do not create separate or additional caps. Nothing limits liability or rights that cannot lawfully be limited, including enforceable Data Subject rights or liability under applicable SCCs or other mandatory transfer clauses.

8.2 Conflicts

Mandatory Applicable Data Protection Laws prevail. For conflicts regarding Processing, the order of precedence is: (i) applicable SCCs and the Mandatory Clauses of the UK Addendum or applicable Swiss adaptations; (ii) this DPA, including its Appendices and Annexes; and (iii) the Service Agreement. Section 8.1.4 governs the application of the Service Agreement's

Confidential

liability terms, subject to non-waivable requirements. The Quebec provisions are part of this DPA, not a separate superior instrument. Non-conflicting terms remain effective.

8.3 **Survival**

The provisions relevant to retained Personal Data survive for as long as the relevant Processing continues. Processor return and deletion obligations are governed by Sections 3.4.4 and 3.4.5; independent Controller retention is governed by Section 4 and Appendix 1. Liability, confidentiality, and other provisions intended by their nature to survive remain effective as applicable. Survival does not authorize additional retention.

8.4 **Amendments**

Supplier may update this DPA to address changes in Applicable Data Protection Laws, the Services, or relevant Processing, provided the update does not materially reduce legally required protection or amend mandatory transfer clauses except as permitted therein. Supplier shall notify Customer of material updates using the contact methods in the Service Agreement. Updates take effect thirty (30) days after notice, or earlier to the extent legally required. Customer may object within that period on specific grounds of material adverse impact, and the Parties shall seek a commercially reasonable resolution. If unresolved, amendments beyond those required by law shall be governed by the Service Agreement's amendment provisions. No update authorizes unlawful Processing.

8.5 **Compensation**

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

8.6 **Non-Assignment**

Assignment of this DPA is governed by the Service Agreement. An assignment does not displace obligations under Applicable Data Protection Laws or applicable transfer clauses, including any required accession or transfer safeguards.

8.7 **Third-Party Rights**

Except as expressly provided in the SCCs, the UK Addendum, the Swiss Addendum, or Applicable Data Protection Laws, this DPA benefits only the Parties and their permitted successors and assigns, and no third party shall have any rights, remedies, or claims under this DPA, whether by contract, statute, or otherwise.

8.8 **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.

8.9 **Integration**

This DPA, together with the Service Agreement and any referenced appendices, annexes, and schedules, constitutes the entire agreement between the Parties regarding Personal Data

Confidential

Processing and supersedes all prior agreements, written or oral, concerning the same. For clarity, all other terms of the Service Agreement remain unchanged.

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 Quebec Private Sector Act. Annex I, Section B also records the nature, purpose, duration, and categories of Processing for purposes of Applicable Data Protection Laws generally, including U.S. state privacy laws.

This Appendix includes:

- **Annex** I: Parties and Data Transfer Details
- **Annex** II: Security Measures
- **Annex** III: Authorized Subprocessors

Subject to Section 8.2, this Appendix supplies details for the relevant Processing and transfers. The body of the DPA governs the allocation of rights, remedies, liability, and the scope of contractual commitments. An Annex does not independently expand those commitments; mandatory requirements of Applicable Data Protection Laws and applicable transfer clauses remain unaffected.

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 Addendum, 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 **(or Processor, where Supplier acts as a Subprocessor)**

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 Addendum, 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, Subprocessor, or Controller, as set out in Section 7.3 of the DPA

B. DESCRIPTION OF THE TRANSFER

Supplier role	Processor or Subprocessor
Categories of Data Subjects	End Users, including Customer's tenants and individuals with whom tenants share digital keys; Customer personnel; and authorized third-party contractors of Customer.
Categories of Personal Data	Identification and contact data (such as name, email address, telephone number); account and unit assignment data; digital credentials and authentication data; device identifiers; access-event records (such as date, time, and access point); End User location data when in close proximity to a Unit and the Services are activated; and support and troubleshooting communications.
Processing purposes and responsibility for lawful bases	Supplier Processes Personal Data on documented Instructions to administer storage-facility access; authenticate users; issue, manage, and revoke digital credentials; record access events; host, operate, maintain, and support the applications and associated interfaces; troubleshoot and correct faults; and maintain security, availability, and service quality, as applicable to the Services purchased. Permitted internal service improvement remains subject to Section 3.6 where the CCPA applies. The relevant Controller determines the lawful basis for this Processing; Customer communicates authorized Instructions where it is itself a Processor. A business-to-business contract does not, by itself, establish contractual necessity as a lawful basis for all affected individuals. Processing required by law is subject to Section 3.2.
Retention	Retention, return, and deletion are governed by Sections 3.4.4 and 3.4.5 and the role-specific criteria in Annex I, Section C.

Supplier role	Independent Controller
Categories of Data Subjects	Customer business contacts and personnel; and End Users, solely to the extent their Personal Data is Processed for the independent Controller purposes described below.
Categories of Personal Data	Depending on the applicable Controller purpose: Customer business-contact names, roles, business contact details, and account correspondence for business-relationship administration and communications; and technical, diagnostic, usage, access-event, and security records for lawful security, analytics, and product-development purposes. End User proximity or location data is not authorized for independent product-development or marketing use merely by inclusion in this DPA; any independent use requires satisfaction of applicable notice, legal-basis, and purpose-limitation requirements. The same data remains subject to the Processor provisions for separate Processing performed on Customer's behalf.
Processing purposes and lawful bases	Independent Controller purposes, where lawful, are managing Supplier's business relationship with Customer and related business communications; protecting Supplier's systems and investigating misuse; developing and improving products and analyzing technical performance and usage; complying with legal obligations; and

Confidential

	establishing, exercising, or defending legal claims. Where recognized and applicable, lawful bases include legitimate interests subject to the legally required assessment, legal obligations, consent where required, or another applicable lawful basis. Marketing is limited to Customer business contacts, subject to legally necessary consent or opt-out mechanisms; this Annex does not authorize marketing to Customer's tenants using entrusted Processor data. These purposes do not convert permitted Service Provider activities into independent Business Processing under the CCPA or override Section 3.6.
Retention	Retention and disposal are governed by the independent Controller criteria in Annex I, Section C.

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 I, Section B.

Categories of personal data transferred

The categories of personal data affected shall include those types of personal data specified in Annex I, 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

Other than End User location data described in Annex I, Section B (which may constitute sensitive Personal Data under certain Applicable Data Protection Laws and is Processed only when the Services are activated and in close proximity to a Unit, subject to the safeguards below), 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.
With respect to such location data, and if any other Sensitive Personal Data is inadvertently Processed or transferred, Supplier shall:

- Apply safeguards appropriate to the sensitivity and risks of the relevant data under Annex II and Applicable Data Protection Laws, including access restrictions, minimization, and encryption where appropriate.
- Limit Processing to what is necessary to provide the Services (e.g., geolocation data used for access control and security purposes).
- Where Supplier becomes aware, in the ordinary course of providing the Services, that it has received Sensitive Personal Data not described in this DPA, use commercially reasonable efforts to notify Customer and to erase such data or handle it in accordance with Customer's Instructions, unless retention is required by Applicable Laws. Nothing in this paragraph obligates Supplier to monitor or inspect Personal Data to identify Sensitive Personal Data.
- Apply additional safeguards required for the relevant Processing by Applicable Data Protection Laws. Customer or the relevant upstream Controller is responsible for legally required notices and consents for Processing on its behalf; Supplier is responsible for those required for its independent Controller Processing.

The frequency of the transfer

Confidential

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 I, Section B.

Purpose(s) of the data transfer and further processing

The purposes of transfers shall include the purposes specified in Annex I, 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. **Processor and Subprocessor Processing:** Retention, return, deletion, and residual backup copies are governed by Sections 3.4.4 and 3.4.5, subject to applicable mandatory requirements, including Section 7.6.5. Customer Instructions and Supplier's own interests do not independently authorize retention beyond those provisions.
2. **Independent Controller Processing:** Supplier retains Personal Data as long as necessary for the lawful purposes identified in Section 4 and this Annex. Applicable legal obligations, the duration of the relevant relationship, and the necessity of establishing, exercising, or defending legal claims determine retention where a lawful basis exists. Supplier shall delete or lawfully anonymize the data when no lawful retention ground remains. Pseudonymization alone does not satisfy deletion or anonymization requirements.

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. For EU GDPR transfers, the competent supervisory authority shall be determined in accordance with Clause 13 of the SCCs and Section 7.3.10 of the DPA.
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 Quebec Private Sector Act transfers, the Commission d'accès à l'information du Québec (CAI) shall be the competent authority.

Confidential

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES

Supplier shall implement and maintain technical and organizational measures appropriate to the risk as required by Applicable Data Protection Laws, taking into account the state of the art, implementation costs, and the nature, scope, context, and purposes of Processing. The measures below apply to the relevant Supplier-controlled systems and Processing; particular implementations may vary by architecture and risk. Supplier may replace a measure with an appropriate alternative that does not materially decrease the overall protection of Personal Data. This Annex does not warrant uninterrupted availability, absolute security, any particular certification, or compliance with an industry framework not expressly agreed in the Service Agreement.

1. **Organizational Controls**
    - Information security policies and procedures appropriate to the nature and risks of the relevant Processing, reviewed and updated as appropriate to material changes and applicable legal requirements.
    - Allocation of responsibility for applicable security and privacy obligations. Particular officer titles, dedicated positions, or organizational structures are required only to the extent mandated by Applicable Data Protection Laws.
    - Security and data-handling instructions or awareness measures appropriate to authorized personnel's access, responsibilities, and the risks of the Processing, including training where appropriate or legally required. No fixed training frequency or curriculum is promised.
    - Procedures for granting, changing, and revoking personnel access appropriate to authorized responsibilities and the risks of the relevant Processing.
2. **Access Controls and Confidentiality**
    - Role-Based Access Control mechanisms, under which access to systems and Personal Data is granted based on the principle of least privilege.
    - Risk-appropriate authentication controls, including multi-factor authentication for privileged administrative and remote access where appropriate to the relevant system and risk, or compensating controls providing appropriate protection.
    - Separation of production, development, and testing access or equivalent controls appropriate to the architecture, data sensitivity, and risk of unauthorized exposure.
    - Authentication and risk-appropriate logging of privileged administrative access to relevant systems.
    - Contractual confidentiality commitments or appropriate statutory confidentiality obligations for personnel authorized to Process Personal Data.
    - Access to Personal Data is limited to individuals with a business need.
3. **Network and System Security**
    - Network segmentation and firewall or equivalent access restrictions appropriate to the hosting architecture and risk.
    - Risk-appropriate endpoint and network protections against malicious activity, including malware protection, detection, or preventive controls as appropriate to the relevant systems.
    - Encryption of Personal Data in transit over public networks using current, industry-recognized protocols, and encryption at rest where appropriate to the data, system, and risk, together with other safeguards necessary to provide legally required security.
    - Controls for encryption-key access, storage, and lifecycle management appropriate to the encryption implementation.
    - Risk-based secure development practices, including code review, security testing, and vulnerability assessment appropriate to relevant software changes and systems.
4. **Monitoring and Incident Response**

- Risk-based monitoring and logging of relevant systems, with alerting and review appropriate to the nature and criticality of the Processing.
- 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 consistent with Section 5.2 of the DPA.
- Supplier maintains procedures designed to investigate security incidents involving Personal Data and to notify Customer of Personal Data Breaches in accordance with Section 5.2 of the DPA.

5. **Data Integrity and Availability**
   - Backup and restoration measures appropriate to the relevant Processing and the risks to Personal Data, including protection against unauthorized access and loss. This provision does not establish a particular backup frequency, storage location, or recovery objective.
   - Recovery and continuity procedures appropriate to the risks of the relevant Processing, including a process for testing, assessing, and evaluating the effectiveness of security measures to the extent required by Applicable Data Protection Laws. No fixed testing frequency, certification, or recovery time is promised.
   - Risk-based vulnerability and patch management, taking account of severity, exploitability, available mitigations, and the relevant systems. No fixed remediation deadline is promised except as expressly agreed or legally required.
   - Availability and recovery arrangements appropriate to the risk, including redundancy where appropriate. Recovery objectives and service levels apply only as expressly agreed in the Service Agreement.
6. **Subprocessor and Vendor Management**
   - Subprocessor contracts and risk-based assessment of safeguards consistent with Section 6 and the requirements applicable to the delegated Processing.
   - Risk-based review of relevant Subprocessor safeguards using available documentation, assessments, reports, or certifications, as appropriate; no separate certification or routine on-site audit of every Subprocessor is promised.
   - Supplier maintains a list of current Subprocessors available to 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**
   - Where Supplier maintains relevant third-party reports or certifications, it shall make the most recent available materials accessible on reasonable written request, subject to confidentiality restrictions and Section 5.3. This provision does not require Supplier to obtain or maintain a certification or commission a report not otherwise expressly agreed.

Confidential

ANNEX III - LIST OF SUBPROCESSORS

The Subprocessor List maintained under Section 6.2 is incorporated into this Annex and identifies the authorized Subprocessors, their delegated Processing functions, and Processing locations to the extent required by Applicable Data Protection Laws or applicable transfer clauses. Customer grants general authorization under Section 6.1; additions and replacements are subject to Sections 6.3 through 6.5.

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.

Janus International France SARL

- Registered Office: 216 Rue de Charenton, 75012 Paris, France
- Principal Place of Business: Same.

Janus International Poland Sp. z o.o. (Janus International Poland Spółka z ograniczoną odpowiedzialnością)

- Registered Office: Graniczna 8E, Building DC4, 54-610 Wrocław, Poland
- 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

Confidential