Digilock Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered into between Security People, Inc. dba Digilock ("**Digilock**") and the Customer ("**Customer**") identified in the associated agreement ("**Agreement**") that governs Customer's use of the SaaS Service. Digilock and Customer may each be referred to as a "Party" and collectively referred to as the "Parties." This DPA is incorporated by reference into the Agreement. All capitalized terms used in this DPA but not defined shall have the meaning set forth in the Agreement. To the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern.

This DPA sets out the terms that apply when Customer Personal Data is Processed by Digilock under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with Applicable Law and respects the rights of individuals whose Personal Data are Processed under the Agreement.

1. Definitions

"**Affiliate**" means an entity that controls, is controlled by or is under common control with the applicable party. For purposes of this definition, "control" means ownership of more than fifty (50%) percent of the voting stock or other ownership interest in an entity.

"**Applicable Law(s)**" means all applicable laws, regulations, and other legal or regulatory requirements in any jurisdiction relating to privacy, data protection/security, or the Processing of Personal Data, including without limitation the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* and its amendments and implementing regulations ("**CCPA**"), privacy laws passed by other U.S. states (together with the CCPA, "**U.S. State Privacy Laws**"), the United Kingdom Data Protection Act 2018, and the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"). For the avoidance of doubt, if Digilock's processing activities involving Personal Data are not within the scope of an Applicable Law, such law is not applicable for purposes of this Addendum.

"**Digilock**" means Security People, Inc., a company incorporated in Texas, and its worldwide affiliates and subsidiaries.

"**Customer Personal Data**" means Personal Data pertaining to Customer's employees, visitors, customers, and other lock users and Processed to provide the Service.

"**EEA**" means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein, as well as, for the purposes of this DPA, Switzerland and the United Kingdom.

"**EU SCCs**" means the Standard Contractual Clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in the "Data Transfers" section below.

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

"**Personal Data**" includes "personal data," "personal information," and "personally identifiable information," and such terms shall have the same meaning as defined by Applicable Law.

"**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making such data available, alignment or combination, restriction, erasure or destruction.

"**Service**" means the services provided by Digilock to Customer as specified in the Agreement.

"**Standard Contractual Clauses**" means the EU SCCs or the UK SCCs, as applicable.

"**UK SCCs**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the Effective Date at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) and completed as described in the "Data Transfers" section below.

2. Relationship of the Parties

2.1. Customer is the data controller as defined under the GDPR and other Applicable Laws, and determines the means and purposes for which Customer Personal Data is Processed by Digilock. To the extent Digilock Processes Customer Personal Data subject to the GDPR or other Applicable Laws, Digilock is a data processor as defined under GDPR and will Process the Customer Personal Data according to the instructions set forth in this DPA, the Agreement and under Applicable Law.

2.2. Customer is a Business and Digilock is a Service Provider, as those terms are defined in the CCPA, of the Customer Personal Data Processed by Digilock subject to the CCPA.

2.3. Digilock hereby certifies that it understands the restrictions and obligations set forth in this DPA and that it will comply with them.

3. Scope and Purposes of Processing

3.1 Purpose Limitation.

(a) Digilock will Process Customer Personal Data solely: (i) to fulfill its obligations to Customer under the Agreement, including this DPA; (ii) on Customer's behalf; and (iii) in compliance with Applicable Laws.
(b) Digilock will not (i) sell or share (as such terms are defined in applicable U.S. State Privacy Laws) Customer Personal Data, (ii) Process Customer Personal Data outside of the direct business relationship between Digilock and Customer, (iii) process Customer Personal Data for any purpose other than for the specific purposes set forth in the Agreement, or (iv) otherwise engage in any Processing of the Customer Personal Data outside of what a processor or Service Provider may engage in under Applicable Law, unless obligated or permitted to do otherwise by Applicable Law.
(c) Digilock shall comply with any applicable restrictions under Applicable Laws on combining the Customer Personal Data with personal data that Digilock receives from, or on behalf of, another person or persons, or that Digilock collects from any interaction between it and any individual.
(d) Further details regarding Digilock's Processing operations, including the purposes for Processing Customer Data, are set forth in Exhibit A.

3.2 Lawful Instructions. Customer will not instruct Digilock to Process Customer Personal Data in violation

of Applicable Law. The Agreement, including this DPA, constitute Customer's complete and final instructions to Digilock regarding the Processing of Customer Personal Data, including for purposes of the Standard Contractual Clauses. Digilock will immediately inform Customer if Digilock is legally required to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions (unless legally prohibited from providing such notice), or if, in Digilock's opinion, an instruction from Customer infringes Applicable Law.

3.3 Notification of Inability to Comply. Digilock will notify Customer within five (5) business days after Digilock makes a determination that it can no longer meet its obligations under Applicable Laws.

3.4 Remediation. Customer shall have the right, upon seven (7) days' notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer Personal Data by Digilock.

4. Limitations on Disclosure

4.1 Digilock will not disclose Customer Personal Data to any third party without first obtaining Customer's written consent, except as provided in Section 5 (Subcontracting), Section 7 (Responding to Individuals Exercising Their Rights Under Applicable Law) or Section 9 (Data Transfers), except as required by law. Digilock will require all employees, contractors and agents that Process Customer Personal Data on Digilock's behalf to protect the confidentiality of the Customer Personal Data and to comply with the other relevant requirements of this DPA.

5. Subcontracting

5.1 Subprocessors. Digilock may subcontract the collection or other Processing of Customer Personal Data only in compliance with Applicable Law and any additional conditions for subcontracting set forth in the Agreement. Customer acknowledges and agrees that Digilock's Affiliates and certain third parties may be retained as subprocessors to Process Customer Personal Data on Digilock's behalf (under this DPA as well as under the Standard Contractual Clauses, if they apply) in order to provide the Service. Digilock's third-party subprocessors are listed at Exhibit B (the "Subprocessor List"). Prior to a subprocessor's Processing of Customer Personal Data, Digilock will impose contractual obligations on the subprocessor substantially the same as those imposed on Digilock under this DPA. Digilock remains liable for its subprocessors' performance under this DPA to the same extent Digilock is liable for its own performance.

5.2 Notification. Digilock shall make available to Customer new subprocessors at least 10 days before authorizing such subprocessor(s) to Process Customer Personal Data in connection with the provision of the Service. The subprocessor agreements may have all commercial information, or provisions unrelated to the Standard Contractual Clauses, redacted prior to sharing with Customer, and Customer agrees that such copies will be provided only upon written request.

5.3 Right to Object. Customer may object to Digilock's use of a new subprocessor on reasonable grounds relating to the protection of Customer Personal Data by notifying Digilock promptly in writing at legal@digilock.com within ten (10) business days after receipt of Digilock's notice in accordance with the mechanism set out in Section 5.2. In its notification, Customer shall explain its reasonable grounds for objection. In the event Customer objects to a new subprocessor, Digilock will use commercially reasonable efforts to make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid Processing of Customer Personal Data by the objected-to new subprocessor without unreasonably burdening Customer. If Digilock is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either Party may terminate without penalty the Processing of

Customer Personal Data and/or the Agreement with respect only to those services which cannot be provided by Digilock without the use of the objected-to new subprocessor by providing written notice to the other Party.

6. Assistance & Cooperation

6.1 Security. Digilock will provide reasonable assistance to Customer regarding Customer's compliance with its security obligations under Applicable Law relevant to Digilock's role in Processing the Customer Personal Data, taking into account the nature of Processing and the information available to Digilock, by implementing reasonable technical and organizational measures without prejudice to Digilock's right to make future replacements or updates to the measures that do not lower the level of protection of Customer Personal Data. Digilock will ensure that the persons Digilock authorizes to Process the Customer Personal Data are subject to written confidentiality agreements or are under an appropriate statutory obligation of confidentiality no less protective than the confidentiality obligations set forth in the Agreement.

6.2 Personal Data Breach Notification & Response. Digilock will comply with the Personal Data Breach-related obligations directly applicable to it under Applicable Law. Taking into account the nature of Processing and the information available to Digilock, Digilock will assist Customer by informing it of a confirmed Personal Data Breach without undue delay or within the time period required under Applicable Law, and in any event no later than seventy-two (72) hours following such confirmation. Digilock will notify Customer at the email address provided in the signature block of the Agreement for purposes of Personal Data Breach notifications. Any such notification is not an acknowledgement of fault or responsibility. To the extent available, this notification will include Digilock's then-current assessment of the following, which may be based on incomplete information:

(a) the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the likely consequences of the Personal Data Breach; and

(c) measures taken or proposed to be taken by Digilock to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

Digilock will provide timely and periodic updates to Customer as additional information regarding the Personal Data Breach becomes available. Customer is solely responsible for complying with legal requirements for incident notification applicable to Customer and fulfilling any third-party notification obligations related to any Customer Data Incident(s). Nothing in this DPA or in the Standard Contractual Clauses shall be construed to require Digilock to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach or other security incidents generally.

7. Responding to Individuals Exercising Their Rights Under Applicable Law

To the extent legally permitted, Digilock shall promptly notify Customer if Digilock receives any requests from an individual seeking to exercise any rights afforded to them under Applicable Law regarding their Personal Data (a "Data Subject Request"). To the extent Customer, in its use of the Service, does not have the ability to address a Data Subject Request, Digilock shall, upon Customer's request, provide commercially reasonable efforts to assist

Customer in responding to such Data Subject Request, to the extent Digilock is legally permitted to do so and the response to such Data Subject Request is required under Applicable Law.

8. DPIAs and Consultation with Supervisory Authorities or other Regulatory Authorities

Upon Customer's written request, Digilock shall provide Customer with reasonable cooperation and assistance as needed and appropriate to fulfill Customer's obligations under Applicable Law to carry out a data protection impact assessment related to Customer's use of the Services. Digilock shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority (as defined under the GDPR) in the performance of its tasks relating the data protection impact assessment, and to the extent required under the Applicable Law.

9. Data Transfers

9.1 Customer authorizes Digilock and its subprocessors to make international transfers of the Customer Personal Data in accordance with this DPA so long as Applicable Law for such transfers is respected.

9.2 With respect to Customer Personal Data transferred from the EEA, the EU SCCs shall apply and form part of this DPA. For purposes of the EU SCCs, they shall be deemed completed as follows:

(a) Customer acts as a controller and Digilock acts as Customer's processor with respect to Customer Personal Data subject to the EU SCCs, and its Module 2 applies.

(b) Clause 7 (the optional docking clause) is not included.

(c) Under Clause 9 (Use of sub-processors), the parties select Option 2 (General written authorization). The initial list of sub-processors is set forth at Exhibit B. Digilock shall update that list at least 10 business days in advance of any intended additions or replacements of sub-processors.

(d) Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

(e) Under Clause 17 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of the Netherlands.

(f) Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of the Netherlands.

(g) Annexes I and II of the EU SCCs are set forth in Exhibit A below.

(h) Annex III of the EU SCCs (List of subprocessors) is inapplicable.

9.3 With respect to Customer Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the UK SCCs shall apply and form part of this DPA. For purposes of the UK SCCs, they shall be deemed completed as follows:

(a) Table 1 of the UK SCCs:

a. The Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in Exhibit A.

b. The Key Contact shall be the contacts set forth in Exhibit A.

(b) Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties pursuant to this Addendum.

(c) Table 3 of the UK SCCs: Annex 1A, 1B, and II shall be set forth in Exhibit A.

(d) Table 4 of the UK SCCs: Either party may end this Addendum as set out in Section 19 of the UK SCCs.

(e) By entering into this DPA, the Parties are deemed to be signing the UK SCCs and their applicable Tables and Appendix Information.

9.4 With respect to Customer Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the EU SCCs shall apply and shall be deemed to have the following differences to the extent required by the Swiss Federal Act on Data Protection ("FADP"):

(a) References to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR.

(b) The term "member state" in the EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs.

(c) References to personal data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.

(d) Under Annex I(C) of the EU SCCs (Competent supervisory authority): where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EU SCCs insofar as the transfer is governed by the GDPR.

10. Audits

Digilock shall allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer subject to the following conditions: so long as the Agreement remains in effect and at Customer's sole expense, Customer may request that Digilock provide it with documentation, data, and records ("Records") no more than once annually relating to Digilock's compliance with this DPA (an "Audit"), except, in the event of a Personal Data Breach occurring on Digilock's systems, Customer will also have the right to conduct an Audit within a reasonable period of time following such Personal Data Breach. To the extent Customer uses a third-party representative to conduct the Audit, Customer shall ensure that such third-party representative is bound by obligations of confidentiality no less protective than those contained in this Agreement. Customer shall provide Digilock with fourteen (14) days prior written notice of its intention to conduct an Audit. Customer shall conduct its Audit in a manner that will result in minimal disruption to Digilock's business operations and shall not be entitled to receive data or information of other clients of Digilock or any other Confidential Information of Digilock that is not directly relevant for the authorized purposes of the Audit. Customer shall reimburse Digilock for any time expended for an Audit at the Digilock's then-current rates, which shall be made available to Customer upon request.

11. Legal Process

If Digilock is legally compelled by a court or other government authority to disclose Customer Personal Data, then to the extent permitted by law, Digilock will promptly provide Customer with sufficient notice of all available details of the legal requirement and reasonably cooperate with Customer's efforts to challenge the disclosure, seek an appropriate protective order, or pursue such other legal action, as Digilock deems appropriate.

12. Return or Destruction of Personal Data

Upon termination of the Agreement and written request from Customer, Digilock shall delete or anonymize Customer Personal Data, unless prohibited by Applicable Law. Nothing will oblige Digilock to delete or anonymize Customer Personal Data from files created for security, backup and business continuity purposes sooner than required by Digilock's data retention processes. If Customer requires earlier deletion of such Customer Personal Data, and such deletion is commercially feasible, Customer must first pay Digilock's reasonable charges for such deletion, which may include costs for business interruptions associated with such a request. If Customer has not requested return or deletion of Customer Personal Data within ninety (90) days from termination of the Agreement, Digilock shall have the right, but not the obligation, to delete or anonymize the Customer Personal Data.

Exhibit A
Annexes I and II of the EU SCCs

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: The exporter is the Customer specified in the Agreement, and their address and contact information are specified in the Agreement.

Address: The address for Customer specified in the Agreement.

Contact person's name, position and contact details: The contact details associated with Customer's account or as otherwise specified in the Agreement.

Activities relevant to the data transferred under these Clauses: Obtaining the Services from Data Importer

Signature and date: By entering the Agreement into which these Standard Contractual Clauses are incorporated, the data exporter will be deemed to have signed these Standard Contractual Clauses as of the date the Agreement is entered.

Role (controller/processor): Controller

Data importer(s):

Name: Security People, Inc. dba Digilock

Address: 9 Willowbrook Court, Petaluma, CA 94954

Contact person's name, position and contact details: The contact details as specified in the Agreement.

Activities relevant to the data transferred under these Clauses: Providing the Services to Data Exporter.

Signature and date: By entering the Agreement into which these Standard Contractual Clauses are incorporated, the data importer will be deemed to have signed these Standard Contractual Clauses as of the date the Agreement is entered.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Customer's employees, visitors, customers, and other lock users.

Categories of personal data transferred

Name, email, telephone number, job role, badge number/RFID credential, lock code/pin.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None anticipated.

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

Continuously, for the length of the Agreement between the parties.

Nature of the processing

Personal data transferred will be processed to (i) provide Digilock services to the data exporter, as set forth in more detail in Section 2.1 in the Agreement, and fulfil the data importer's obligations under the Agreement; and (ii) compliance with applicable law.

Purpose(s) of the data transfer and further processing

Personal data transferred will be processed to (i) provide Digilock services to the data exporter, as set forth in Section 2.1 in the Agreement, and fulfil the data importer's obligations under the Agreement; and (ii) compliance with applicable law.

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

Personal data shall be retained for the length of time necessary to provide Digilock services under the Agreement, or as otherwise required by applicable law.

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

Digilock's subprocessors will process personal data to assist Digilock in providing the Digilock services pursuant to the Agreement, for as long as needed for Digilock to provide the Digilock services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13.

The parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Dutch Data Protection Authority.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

Digilock's security measures are outlined in its SOC 2 Type 2 report, which is available on demand.

Exhibit B
Digilock Subprocessors

Amazon Web Services

Heroku

Auth0