

flock safety

FLOCK API AND INTEGRATIONS POLICY

This Flock API and Integrations Policy (“**Terms**”) describes your (“**You**” or “**Your**” or the “**City**”) obligations when accessing or using the Flock Group, Inc. (“**Flock**” or “**our**”) application programming interface (“**API**” or “**APIs**”, defined below) and integrations (“**Integrations**”) (collectively “**Implementation**”). By accessing this Implementation, You (as a “**Party**,” and together with Flock, the “**Parties**”), agree to comply with these terms, and shall only use the Implementation for bona fide law enforcement purposes (“**Purpose**”).

In these Terms:

- “**API**” or “**APIs**” means Flock’s application programming interface and any programming interface and any accompanying or related documentation, source code, SDKs, executable applications and other materials made available by Flock.
- “**Data**” means any content, documentation, material, vehicle images, video, audio, attributes, date, time, location, or anything derivative thereof that is either requested to be sent or received through the Implementation, at the express instruction of a Flock Customer.
- “**Flock Customer**” means a customer of Flock services which has signed Flock’s terms and conditions (“**Customer Agreement**”) and is currently requesting integration with this Implementation (“**Customer Authorization**”).
- “**Hotlist(s)**” means a digital file containing alphanumeric license plate related information pertaining to vehicles of interest, which may include stolen vehicles, stolen vehicle license plates, vehicles owned or associated with a wanted or missing person(s), vehicles suspected of being involved with criminal or terrorist activities, and other legitimate law enforcement purposes. Hotlists also include, but are not limited to, national data (i.e., NCIC) and similar categories, license plates associated with AMBER Alerts or Missing Persons/Vulnerable Adult Alerts, and manually entered license plate information associated with crimes that have occurred in any local jurisdiction.
- “**Integration**” or “**Integrations**” means the code which Parties may transfer Data and other information between systems.

1. Use and Restriction

1.1 Registration. To access certain Implementations You may be required to provide certain information (such as identification or contact details) as part of the registration process for access or continued use of the Implementation. Any registration information You give to Flock shall always be accurate and current. You shall promptly inform Flock of any updates.

1170 Howell Mill Rd. NW · Suite 210, Atlanta, GA 30318

flock safety

1.2 Restrictions. Flock owns all right, title and interest in the Implementation. You only receive rights to use the Implementation as granted by these Terms. You understand that such Implementation may provide limited access to certain kinds of Data, as applicable, and shall be accessed strictly in accordance with these Terms and all applicable laws. Where any personally identifiable information is being exchanged, Parties agree to sign a data processing addendum which appropriately outlines each Parties compliance obligations, as applicable. Further, access to Flock's Implementation may enable You to activate sharing notifications to be used by a CJIS compliant entity, as applicable, for the Purpose. You shall comply with all applicable restrictions set forth in these Terms, including the Privacy Policy (<https://www.flocksafety.com/privacy-policy>), in all uses of the Implementation. Your access to the Implementation is limited to the enablement of Implementation, of which must be authorized by and instructed upon by a Flock Customer. You shall not, nor permit others, whether directly or indirectly, to: (i) use the Implementation in any manner that violates any applicable laws or these Terms (ii) use the Implementation in any manner that infringes, misappropriates, or violates any third party's rights, (iii) use or manipulate the Implementation for machine learning model development or evaluation, (iv) meddle with, reverse assemble, reverse compile, decompile, translate, engage in model extraction, attempt to discover underlying components (including source code) or any part of the software or any products supplied as a part of these Terms, (v) access, use or share any data from the Implementation, including derivative data, for any reason other than as such permitted under these Terms, (vi) buy, sell or transfer any API keys of Integration access tools or code, or (vii) sell or share any Data, unless expressly authorized in writing by the appropriate data owner or licensor. If Flock believes, in its sole discretion, that You have violated or attempted to violate any term, condition or any spirit of these Terms, such action is considered a material breach, and any license afforded to You pursuant to these Terms may be temporarily or permanently revoked, with or without notice to You.

1.3 Damages. To the extent not inconsistent with all principles of sovereign immunity, Flock is entitled to seek all direct losses incurred as a result of the breach of Terms by You, including, but not limited to, lost revenue, software downtime, and reasonable costs associated with the enforcement of these Terms, including legal fees. To the extent not inconsistent with all principles of sovereign immunity, You acknowledge that Flock may seek the remedies of both monetary damages and equitable relief, including injunctive relief to prevent ongoing or further breaches. However, Flock will make reasonable efforts to mitigate any damages resulting from Your breach of these Terms. It is the intent of this clause to fairly compensate Flock without penalizing You beyond what is necessary to make Flock whole.

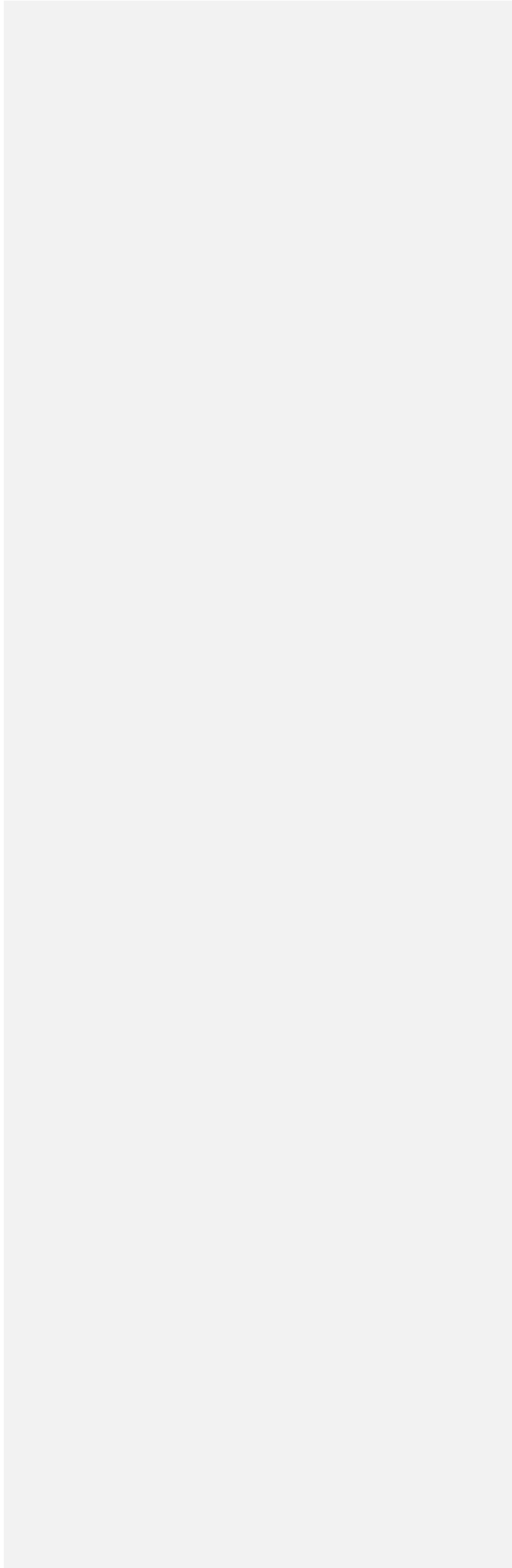
1. Implementation License. Subject to these Terms, Flock grants You a limited, non-exclusive, non-transferable, non-sublicensable, revocable right to access the Implementation to the limited extent that such is requested by a Flock Customer. Further, Flock shall have, and You shall hereby grant to Flock, a royalty-free, fully paid-up, worldwide, transferable, sub-licensable, irrevocable and perpetual license to implement, use, modify, commercially exploit, incorporate into any of Flock's products or services and/or otherwise use in any manner any suggestions, enhancement requests, recommendations or other feedback Flock receives from You.

2. Confidentiality. You may from time to time obtain access to Flock's proprietary information as a result of this engagement. You shall use proprietary information only to the extent necessary to exercise its rights under these Terms. Subject to the express permissions set forth herein, You shall not disclose proprietary information to a third party without the prior express written consent of Flock. Without limiting any of Your obligations under these Terms, You agree that You shall protect proprietary information from unauthorized use, access, or disclosure in the same manner that You would use to protect Your own confidential and proprietary information of a similar nature and in any event with no less than a reasonable degree of care.

3. Your Representations and Warranties.

3.1 Representation. You represent, covenant, and warrant that You shall use the Implementation only in compliance with these Terms and all applicable laws and regulations, including but not limited to any laws relating to the recording or sharing of video, photo, or audio content.

1170 Howell Mill Rd. NW · Suite 210, Atlanta, GA 30318



flock safety

3.2 Warranty. You understand that Flock offers this Implementation “as is” and without warranty of any kind, express or implied, and subject to these Terms. Flock has no obligation to maintain, correct, update, change, modify, or otherwise support the Implementation. Flock may discontinue providing access to the Implementation at any time (without notice). Flock makes no guarantee, representation, or commitment as to the success, quality, or intended use case of this Implementation.

4. Limitation of Liability.

4.1 Limitation on Direct Damages. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL FLOCK, ITS OFFICERS, DIRECTORS, AGENTS, EMPLOYEES OR REPRESENTATIVES BE LIABLE FOR ANY AMOUNT GREATER THAN THE FEES PAID BY YOU TO FLOCK UNDER THESE TERM, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), PRODUCT LIABILITY OR OTHERWISE.

4.2 Waiver of Consequential Damages. IN NO EVENT SHALL FLOCK OR ITS LICENSORS OR SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA OR LOSS OF PROFITS, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

4.3 No Waiver of Sovereign Immunity. Notwithstanding any provision to the contrary herein or any other policies, terms and/or conditions that may apply to this agreement, the City does not waive any forms of sovereign immunity and expressly reserves same.

5. Termination for Convenience. You may stop using the Implementation at any time with or without notice to Flock. If You want to terminate these Terms, You must provide Flock with prior written notice and, upon termination, stop using the Implementation. Flock may terminate Your access to the Implementation or these Terms at any time without further obligation to You. Upon termination, You shall immediately: stop using the Implementation; return or destroy all of our confidential information; delete any cached or stored content that was permitted by the Terms; and, upon Flock's request, confirm to Flock in writing that You have fulfilled Your obligations pursuant to this section.

6. Entire Understanding. Parties understand that Flock may, from time to time, update these Terms. Consistent with section 10 below, Flock will provide written notice of any such material update(s) to promptly upon implementation. Notwithstanding, these Terms contain the entire understanding between Parties as it pertains to the Implementation and supersede all prior and contemporaneous terms, understandings, express or implied, oral or written, of any nature with respect to the subject matter hereof.

7. Assignment; Successors. You cannot, without our prior written consent, assign these Terms. These Terms shall bind the Parties and their respective successors and permitted assigns. Any assignment in contravention of this subsection shall be void. For purposes of the Terms and for the avoidance of doubt, “assign” shall also include any assignment to a successor in interest who obtains all or substantially all of the assigning Party's assets through consolidation, merger or acquisition.

Commented [KN1]: Rejected. Flock will not accept 5M for liability around Flock's API policy. Such increase is disproportionate to the circumstances.

8. Relationship. No agency, partnership, joint venture, or employment is created as a result of these Terms and Parties do not have any authority of any kind to bind each other in any respect whatsoever. Flock shall at all times be and act as an independent contractor to You.

9. Notices. All notices under these Terms will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested. All notices will be provided to the email or mailing address listed on the applicable order form or the email address associated with You.

1170 Howell Mill Rd. NW · Suite 210, Atlanta, GA 30318

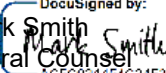
flock safety

10. Modifications. Parties understand that Flock must be able to modify these Terms from time to time in order to comply with new software, laws, and/or compliance requirements. However, Flock will post such updated Terms on our website at the following link (<http://flocksafety.com/api-integration-policy>), which modification(s) will become effective immediately. You will be promptly informed of any material changes. By continuing to use and access this Implementation, you agree to comply with such updated Terms. If you do not agree with the updated terms, Flock asks you to discontinue use of the Implementation immediately.

Commented [KN2]: Re-inserted. Respectfully, Flock is constantly updating its software and terms in order to keep up with compliance laws and regulations. If you do not agree with the updated terms, Flock asks you to discontinue use immediately.

By signing below, Parties acknowledge that they have read and understand the above terms and conditions.

Flock Group Inc

DocuSigned by:
Name: Mark Smith
Title: General Counsel
Signature: 
AC5C931454C24F3

Date:

You [entity name] :
Chief Mike Carlson

Name:
Title:
Signature:

Date:

1170 Howell Mill Rd. NW · Suite 210, Atlanta, GA 30318



DATA PROCESSING AGREEMENT

PARTIES AND BACKGROUND

- (A) The customer ("**Customer**") agreeing to this Data Processing Agreement (the "**DPA**") has entered into an agreement with Flock Group, Inc. ("**Flock**") (each a "**Party**" and collectively the "**Parties**") under which Flock has agreed to provide the services in accordance with such underlying agreement (the "**Agreement**"). This DPA is incorporated into and forms part of the Agreement and shall be effective and replace any previously applicable data processing and security terms as of the date the DPA is executed by the Parties ("**Effective Date**").
- (B) To the extent that Flock processes any Customer Personal Data (as defined below) on behalf of the Customer (or, where applicable, the Customer Affiliate) in connection with the provision of the Services, the Parties have agreed to do so in accordance with the terms of this DPA.

1. DEFINITIONS

1.1 Capitalised terms used but not defined within this DPA shall have the meaning set forth in the Agreement. The following capitalised terms used in this DPA shall be defined as follows:

"**Affiliate**" means an entity that, directly or indirectly, owns or controls, is owned or is controlled by, or is under common ownership or control with a Party and is a beneficiary of the Agreement;

"**Approved Addendum**" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Mandatory Clauses;

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the Effective Date of this DPA;

"**Customer Personal Data**" means the Personal Data processed by Flock on behalf of Customer or Customer Affiliate in connection with the provision of the Services;

"**EEA**" means the European Economic Area;

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 or, where applicable, the equivalent provision under Swiss data protection law;

"**Mandatory Clauses**" means "Part 2: Mandatory Clauses" of the Approved Addendum;

"**Member State**" means a member state of the EEA, being a member state of the European Union, Iceland, Norway, or Liechtenstein;

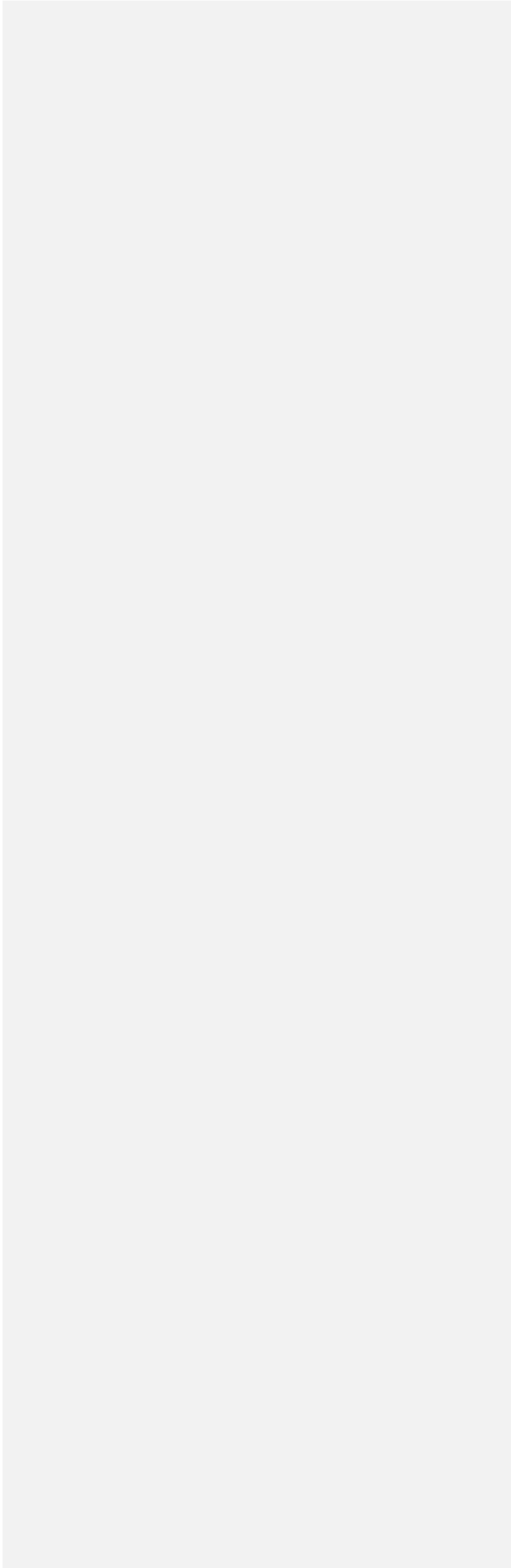
"**Personal Data**" means any information relating to an identified or identifiable individual or device, or is otherwise "**personal data**," "**personal information**," "**personally identifiable information**" and similar terms, and such terms shall have the same meaning as defined by applicable data protection laws;

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to (including unauthorised internal access to), Customer Personal Data;

"**Standard Contractual Clauses**" or "**SCCs**" means Module Two (*controller to processor*) and/or Module Three (*processor to processor*) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914;

"**Sub-processor**" means Flock Affiliates and third-party processors appointed by Flock to process Customer Personal Data; and

"UK" means the United Kingdom of Great Britain and Northern Ireland.



Docusign Envelope ID: 39C4A31B-1980-4CBF-A6E9-4A6FEA0FB976

- 1.2 The terms "**controller**", "**processor**", "**data subject**", "**process**", and "**supervisory authority**" shall have the same meaning as set out in the GDPR.
- 1.3 The terms "**sell**" and "**service provider**" shall have the same meaning as set out in the CCPA.

2. INTERACTION WITH THE AGREEMENT

- 2.1 This DPA supplements and (in case of contradictions) supersedes the Agreement with respect to any processing of Customer Personal Data.
- 2.2 With respect to Customer Affiliates, by entering into this DPA Customer warrants it is duly authorised to enter into this DPA for and on behalf of any such Customer Affiliates and, subject to clause 2.3, each Customer Affiliate shall be bound by the terms of this DPA as if they were the Customer. Notwithstanding, Customer shall be liable for any and all Customer Affiliates actions in connection with this DPA as if those actions were those of the Customer.
- 2.3 Customer warrants that it is duly mandated by any Customer Affiliates on whose behalf Flock processes Customer Personal Data in accordance with this DPA, to (a) enforce the terms of this DPA on behalf of the Customer Affiliates, and to act on behalf of the Customer Affiliates in the administration and conduct of any claims arising in connection with this DPA; and (b) receive and respond to any notices or communications under this DPA on behalf of Customer Affiliates.
- 2.4 The Parties agree that any notice or communication sent by Flock to Customer shall satisfy any obligation to send such notice or communication to a Customer Affiliate.

2.5 Notwithstanding anything to the contrary in the Agreement, Customer shall indemnify Flock from and against all and any losses that are sustained, suffered or incurred by, awarded against or agreed to be paid by the other parties to the extent arising from Customer's breach of its obligations under this Agreement and/or failure to comply with all applicable data protection laws.

2.6 Notwithstanding anything to the contrary herein, Flock and its affiliates total liability for any and all claims pursuant this DPA, including any and all damages or liability of any type pertaining to a breach of this DPA, in the aggregate, shall not exceed one million dollars (\$1,000,000.00).

3. ROLE OF THE PARTIES

- 3.1 The Parties acknowledge and agree that:
- (a) for the purposes of the GDPR, Flock acts as "processor" or "sub-processor." Flock's function as processor or sub-processor will be determined by the function of Customer:
- (i) In general, Customer functions as a controller, whereas Flock functions as a processor.
 - (ii) In certain cases, Customer functions as a processor on behalf of Customer's Customers where Customer and Customer's Customer have concluded a data processing agreement in relation to the processing of Personal Data of Customer's Customers; and
- (b) for the purposes of the CCPA, Flock will act as a "service provider" in its performance of its obligations pursuant to the Agreement.

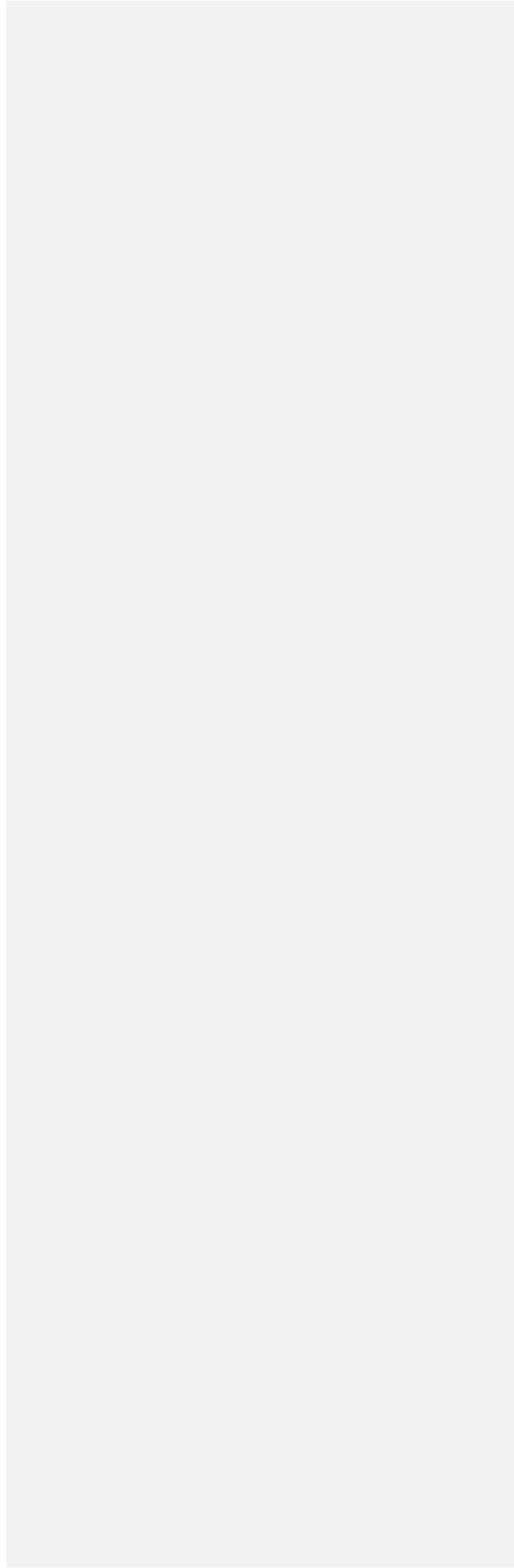
4. DETAILS OF DATA PROCESSING

- 4.1 The details of data processing (such as subject matter, nature and purpose of the processing, categories of Personal Data and data subjects) are described in the Agreement and in Schedule 1, in addition to Flock's privacy policy (<https://www.flocksafety.com/privacy-policy>), which is incorporated herein by reference.
- 4.2 Customer Personal Data will only be processed on behalf of and under the instructions of Customer and in accordance with applicable law. The Agreement and this DPA shall be Customer's instructions for the processing of Customer Personal Data.

Commented [KN3]: Language re-inserted. Flock will not take on liability for Customer's breach of terms. Furthermore, Flock can not accept unlimited liability and therefore must have a cap for potential damages. It is industry standard for companies to ensure liability is proportionate to the services provided and Flock feels 1M is an appropriate cap.

4.3 If Customer's instructions will cause Flock to process Customer Personal Data in violation of applicable law or outside the scope of the Agreement or the DPA, Flock shall promptly inform Customer thereof, unless prohibited by applicable law (without prejudice to the SCCs).

2



DocuSign Envelope ID: 39C4A31B-1980-4CBF-A6E9-4A6FEA0FB976

- 4.4 Flock is permitted to anonymize Customer Personal Data through a reliable state of the art anonymization procedure and use such anonymized data for its own business purposes, including for research, development of new products and services, and security purposes.
- 4.5 Flock may store and process Customer Personal Data anywhere Flock or its Sub-processors maintain facilities, subject to clause 5 of this DPA.

5. SUB-PROCESSORS

- 5.1 Customer grants Flock general authorisation to engage Sub-processors, subject to clause 5.2, as of the Effective Date.
- 5.2 Flock shall (i) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data than Flock's obligations under this DPA to the extent applicable to the nature of the services provided by such Sub-processor.
- 5.3 Flock shall provide Customer with at least fifteen (15) days' notice of any proposed changes to the Sub-processors it uses to process Customer Personal Data (including any addition or replacement of any Sub-processors). Customer may object to Flock's use of a new Sub-processor (including when exercising its right to object under clause 9(a) of the SCCs) by providing Flock with written notice of the objection within ten (10) days after Flock has provided notice to Customer of such proposed change (an "**Objection**"). In the event Customer objects to Flock's use of a new Sub-processor, Customer and Flock will work together in good faith to find a mutually acceptable resolution to address such Objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, either party may, as its sole and exclusive remedy, terminate the Agreement by providing written notice to the other party. During any such Objection period, Flock may suspend the affected portion of the Services.

6. DATA SUBJECT RIGHTS REQUESTS

- 6.1 As between the Parties, Customer shall have sole discretion and responsibility in responding to the rights asserted by any individual in relation to Customer Personal Data ("**Data Subject Request**").
- 6.2 Flock will forward to Customer without undue delay any Data Subject Request received by Flock or any Sub-processor from an individual in relation to their Customer Personal Data and may advise the individual to submit their request directly to Customer.
- 6.3 Flock will (taking into account the nature of the processing of Customer Personal Data) provide Customer with self-service functionality through the Services or other reasonable assistance as necessary for Customer to fulfil its obligation under applicable law to respond to Data Subject Requests, including if applicable, Customer's obligation to respond to requests for exercising the rights set out in the GDPR or CCPA. Flock may charge Customer, and Customer shall reimburse Flock, for any such assistance beyond providing self-service features included as part of the Services.

7. SECURITY AND AUDITS

- 7.1 Flock will implement and maintain appropriate technical and organisational data protection and security measures designed to ensure security of Customer Personal Data, including, without limitation, protection against unauthorised or unlawful processing (including, without limitation, unauthorised or unlawful disclosure of, access to and/or alteration of Customer Personal Data) and against accidental loss, destruction, or damage of or to it.
- 7.2 Flock will implement and maintain as a minimum standard the measures set out in Schedule 2. Flock may update or modify the security measures set out in Schedule 2 from time to time, including (where applicable) following any review by Flock of such measures in accordance with clause 8.6 of the SCCs, provided that such updates and/or modifications do not reduce the overall level of protection afforded to the Customer Personal Data by Flock under this DPA.
- 7.3 Customer or its independent third-party auditor reasonably acceptable to Flock (which shall not include any

auditors who are not suitably qualified or independent or are a competitor of Flock) may audit Flock's compliance with its obligations under this DPA up to once per year, or more frequently in the event a Security Incident has

Docusign Envelope ID: 39C4A31B-1980-4CBF-A6E9-4A6FEA0FB976

occurred or to the extent required by applicable data protection laws, including where mandated by Customer's regulatory or governmental authority.

- 7.4 To request an audit, Customer must submit a detailed proposed audit plan to Flock at least two weeks in advance of the proposed audit date. Flock will review the proposed audit plan and work cooperatively with Customer to agree on a final audit plan. All such audits must be conducted during regular business hours, subject to the agreed final audit plan and Flock's health and safety or other relevant policies, and may not unreasonably interfere with Flock business activities. Nothing in this clause 7.4 shall require Flock to breach any duties of confidentiality.
- 7.5 If the requested audit scope is addressed in an ISO 27001 certification, SOC 2 Type 2 report or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Flock confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.
- 7.6 Customer will promptly notify Flock of any non-compliance discovered during the course of an audit and provide Flock any audit reports generated in connection with any audit, unless prohibited by applicable law or otherwise instructed by a regulatory or governmental authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA.
- 7.7 Any audits are at Customer's expense. Customer shall reimburse Flock for any time expended by Flock or its Sub-processors in connection with such audits.
- 7.8 Flock shall audit its Sub-processors on a regular basis and will, upon Customer's request, confirm their compliance with data protection law and the obligations set upon Sub-processors according to the data processing agreement concluded with them. Customer may request Flock to conduct further audits only in the event reasonably justified, and in such cases Flock will conduct further audits to the extent permissible.

8. SECURITY INCIDENTS

Flock will promptly notify Customer in writing in the event of any breach of this DPA, applicable law or any instruction by Customer in connection with the processing of Customer Personal Data under this DPA. Without limiting the generality of the foregoing, Flock shall notify Customer in writing without undue delay after becoming aware of any Security Incident, and reasonably cooperate in the investigation of any such Security Incident and any obligation of Customer under applicable law to make any notifications to individuals, supervisory authorities, governmental or other regulatory authority, or the public in respect of such Security Incident. Flock shall take reasonable steps to contain, investigate, and mitigate any Security Incident, and shall, without undue delay, send Customer timely information about the Security Incident, including, but not limited to, the nature of the Security Incident, the measures taken to mitigate or contain the Security Incident, and the status of the investigation. Flock's notification of or response to a Security Incident under this clause 8 will not be construed as an acknowledgement by Flock of any fault or liability with respect to the Security Incident.

9. DELETION AND RETURN

Flock shall, within 90 days of the date of termination or expiry of the Agreement, (a) if requested to do so by Customer within that period, return a copy of all Customer Personal Data or provide self-service functionality allowing Customer to do the same; and (b) delete and use all reasonable efforts to procure the deletion of all other copies of Customer Personal Data processed by Flock or any Sub-processors. Notwithstanding, this is only applicable to Customer Personal Data within Flock's possession at the time of the request.

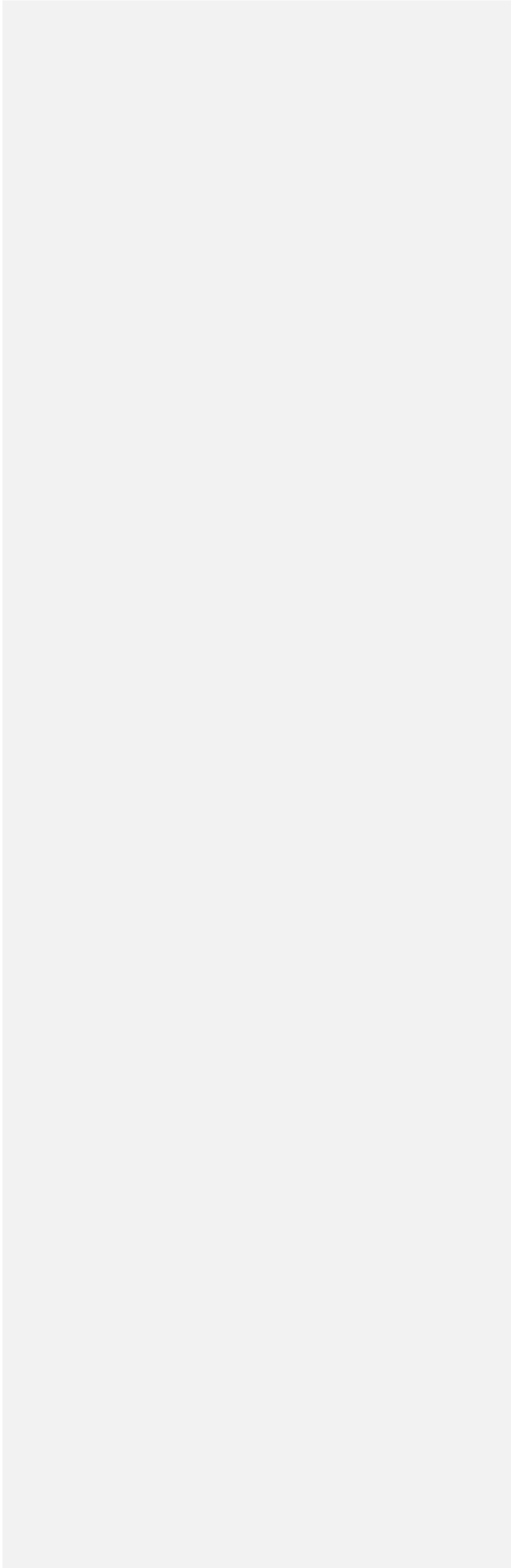
10. CONTRACT PERIOD

This DPA will commence on the Effective Date and, notwithstanding any termination of the Agreement, will remain in effect until, and automatically expire upon, Flock's deletion of all Customer Personal Data as described in this DPA.

11. STANDARD CONTRACTUAL CLAUSES

The Parties agree that the terms of the Standard Contractual Clauses Module Two (Controller to Processor) and Module Three (Processor to Processor), as further specified in Schedule 3 of this DPA, are hereby incorporated by

4



Docusign Envelope ID: 39C4A31B-1980-4CBF-A6E9-4A6FEA0FB976

reference and shall be deemed to have been executed by the Parties and apply to any transfers of Customer Personal Data falling within the scope of the GDPR from Customer (as data exporter) to Flock (as data importer).

12. SUPPORT FOR CROSS-BORDER DATA TRANSFERS

If applicable, Flock will provide Customer reasonable support to enable Customer's compliance with the requirements imposed on the transfer of personal data to third countries with respect to data subjects located in the EEA, Switzerland, and UK. Flock will, upon Customer's request, provide information to Customer which is reasonably necessary for Customer to complete a transfer impact assessment ("TIA"). Flock further agrees to implement the supplementary measures agreed upon and set forth in Schedule 4 of this DPA in order to enable Customer's compliance with requirements imposed on the transfer of personal data to third countries. Flock may charge Customer, and Customer shall reimburse Flock, for any assistance provided by Flock with respect to any TIAs, data protection impact assessments or consultation with any supervisory authority of Customer.

13. CUSTOMER PERSONAL DATA SUBJECT TO THE UK AND SWISS DATA PROTECTION LAWS

To the extent that the processing of Customer Personal Data is subject to UK or Swiss data protection laws, the UK Addendum and/or Swiss Addendum (as applicable) set out in Schedule 5 shall apply.

14. CUSTOMER PERSONAL DATA SUBJECT TO THE CCPA

14.1 If Customer or Customer Affiliates provide Flock any Customer Personal Data that is "personal information" under the CCPA, Flock will:

- (a) act as a service provider with regard to such personal information;
- (b) retain, use, and disclose such personal information solely for the purpose of performing the Services or as otherwise permitted under the CCPA;
- (c) not sell Customer Personal Data to another business or third party. Notwithstanding the foregoing, disclosures to a third party in the context of a merger, acquisition, bankruptcy, or other transaction shall be permitted in accordance with the terms of the Agreement; and
- (d) provide reasonable assistance to Customer in responding to requests from consumers pursuant to the CCPA with regard to their personal information, and in accordance with clause 6 of this DPA.

14.2 Flock certifies that it understands the foregoing obligations and shall comply with them for the duration of the Agreement and for as long as Flock processes Customer Personal Data.

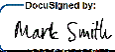
[Signature Page Follows]

DocuSign Envelope ID: 39C4A31B-1980-4CBF-A6E9-4A6FEA0FB976

In Witness Whereof, the parties hereto have caused this Data Processing Agreement to be executed by their duly authorised representatives as of the Effective Date.

FLOCK GROUP, INC.

Customer:

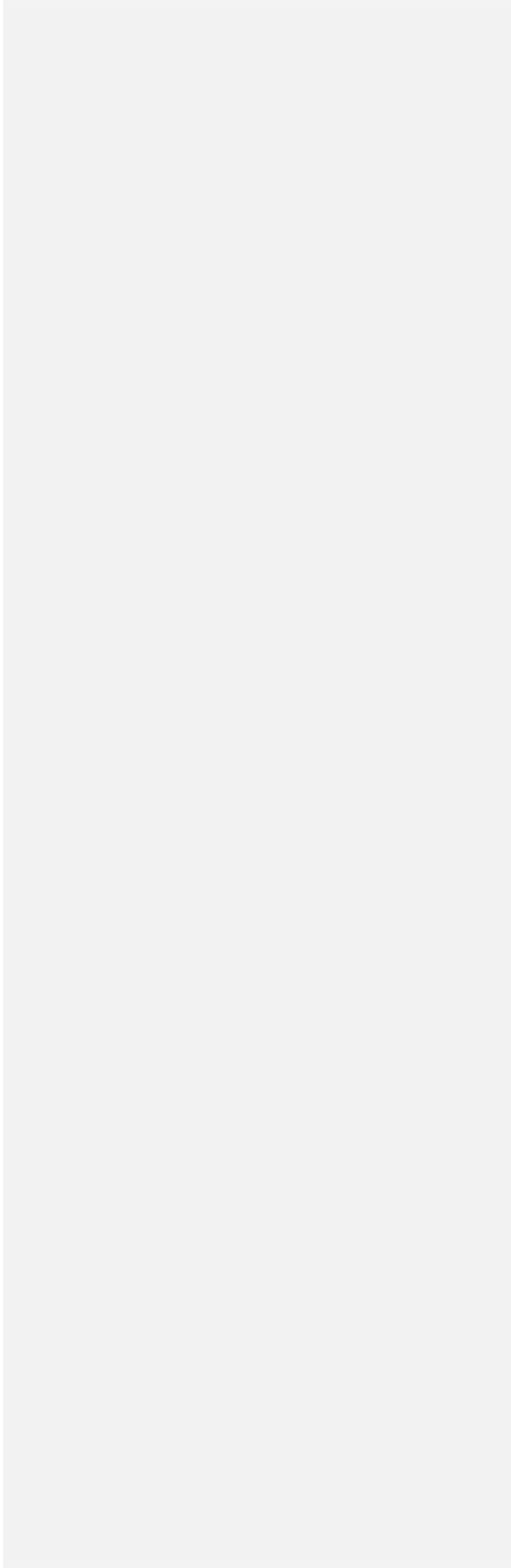
By:  By: _____

Mark Smith

Name: _____

Date: 6/17/2024

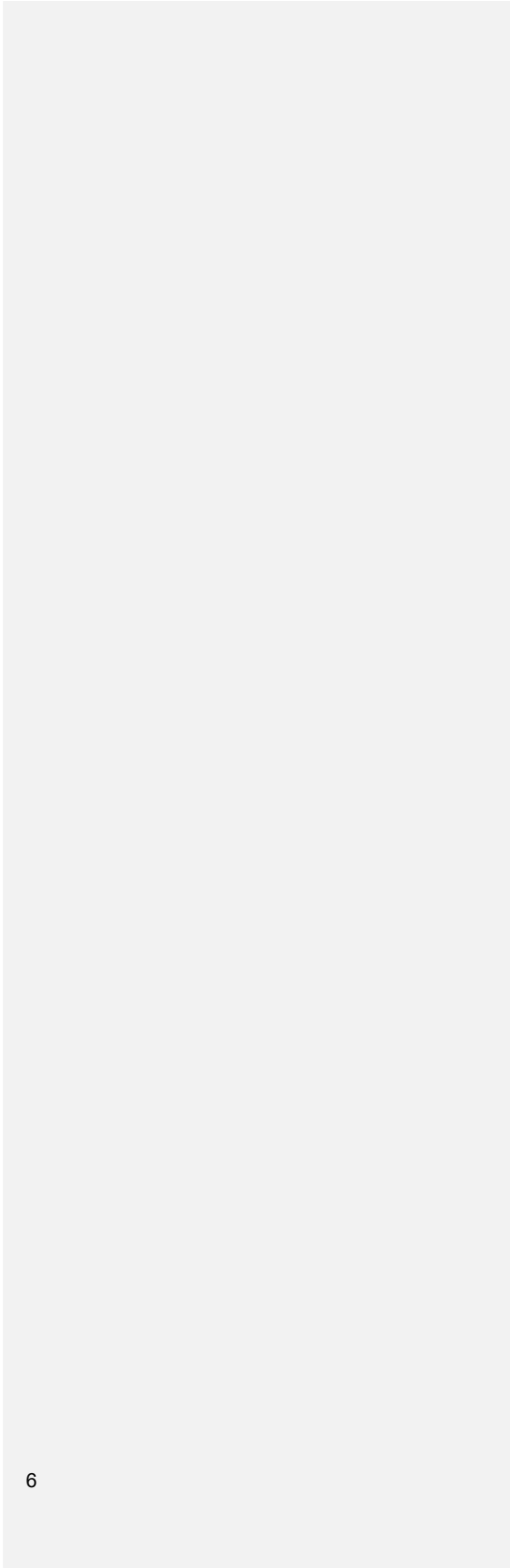
Title: General Counsel



Chief Mike Carlson
Name: _____

Title: _____

Date:



DocuSign Envelope ID: 39C4A31B-1980-4CBF-A6E9-4A6FEA0FB976

SCHEDULE 1

DETAILS OF PROCESSING

A. List of Parties

1. Data Exporter

Customer and/or the Customer Affiliates.

2. Data Importer

Flock Group, Inc.

Attn: Privacy

1170 Howell Mill Road NW Suite 210

Atlanta, GA 30318

Attn: Privacy Legal

The data importer's contact person can be contacted at privacy@flocksafety.com.

The data importer's activities relevant to the data transfer under these clauses are as follows: the data importer processes personal data provided by the data exporter on behalf of the data exporter in connection with providing the Services to the data exporter as further specified in the Agreement.

B. Description of Transfer

1. Categories of data subjects

The categories of data subjects whose personal data are transferred: *Multiple/natural persons within Customer or Customer Affiliate's region of Services, subject to the Agreement.*

2. Categories of personal data

The transferred categories of personal data are: *Determined by Customer's configuration of the Services, and may include name, phone number, age/birthday, email address, address data, IP address, device identifiers, licence plates, usage data (such as interactions between a user and Flock's online system, website or email, used browser, used operating system, referrer URL).*

Moreover, Customer and Customer Affiliate may include further personal data of data subjects as specified above (in particular in unstructured form) in connection with their use of the Services according to the Agreement.

3. Special categories of personal data (if applicable)

The transferred personal data includes the following special categories of data: *N/A*

The 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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures are: *N/A*

4. Frequency of the transfer

The frequency of the transfer is: *The transfer is performed on a continuous basis and is determined by Customer's configuration of the Services.*

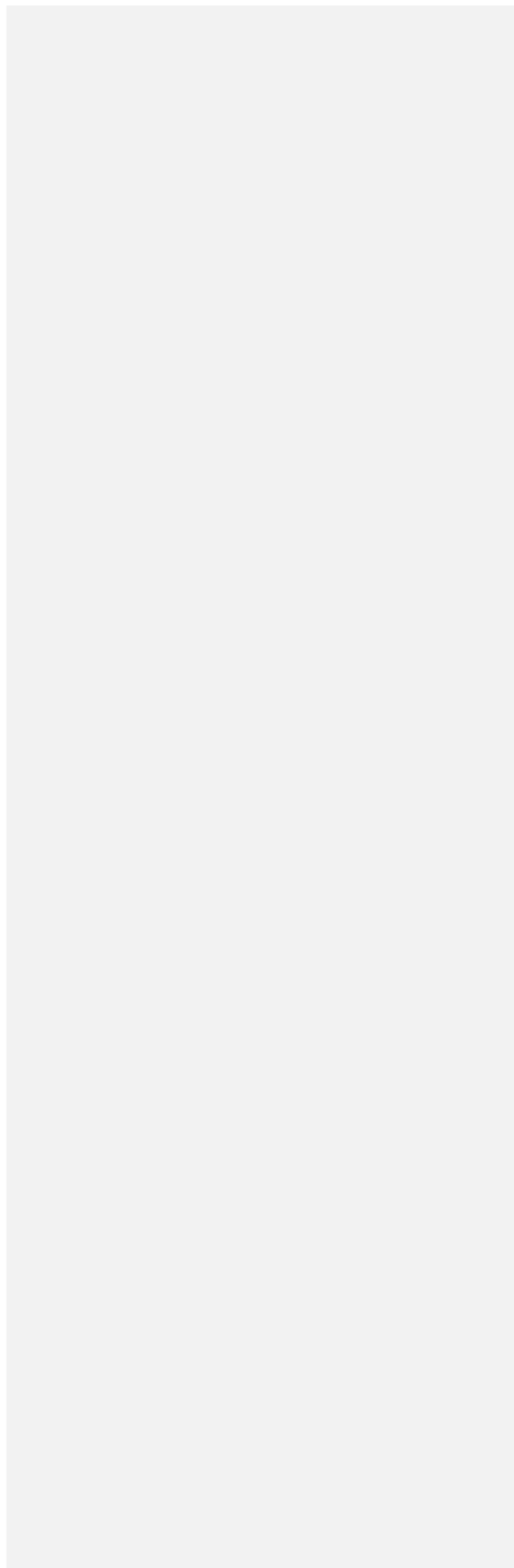
5. Subject matter and nature of the processing

The subject matter of the processing is: *to provide data integration into Flock's SaaS platform as described in the Agreement.*

6. Purpose(s) of the data transfer and further processing

The purpose/s of the data transfer and further processing is: *to provide the Services to Customer pursuant to the Agreement so to enhance its Customer relationships and improve Flock's government user experience.*

7



7. Duration

Unless otherwise specified in the Agreement, the period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: *the duration is defined in clause 10 of the DPA.*

8. Sub-processor (if applicable)

For transfers to sub-processors, specify subject matter, nature, and duration of the processing: *as stipulated in clause 5.1 of the DPA. The Sub-processors may have access to the Personal Data for the term of this DPA or until the service contract with the respective Sub-processor is terminated or the access by the Sub-processor has been excluded as agreed between Flock and Customer.*

9. Recipient

Customer hereby authorises Flock to send Customer Personal Data to the following recipient(s) in accordance with this DPA:

Brookhaven GA Police Department address

Chamblee GA Police Department

Sandy Springs GA Police Department

Dekalb Co Police Department

Gwinnett Co GA Police Department

Doraville GA Police Department

Cobb Co GA Police Department

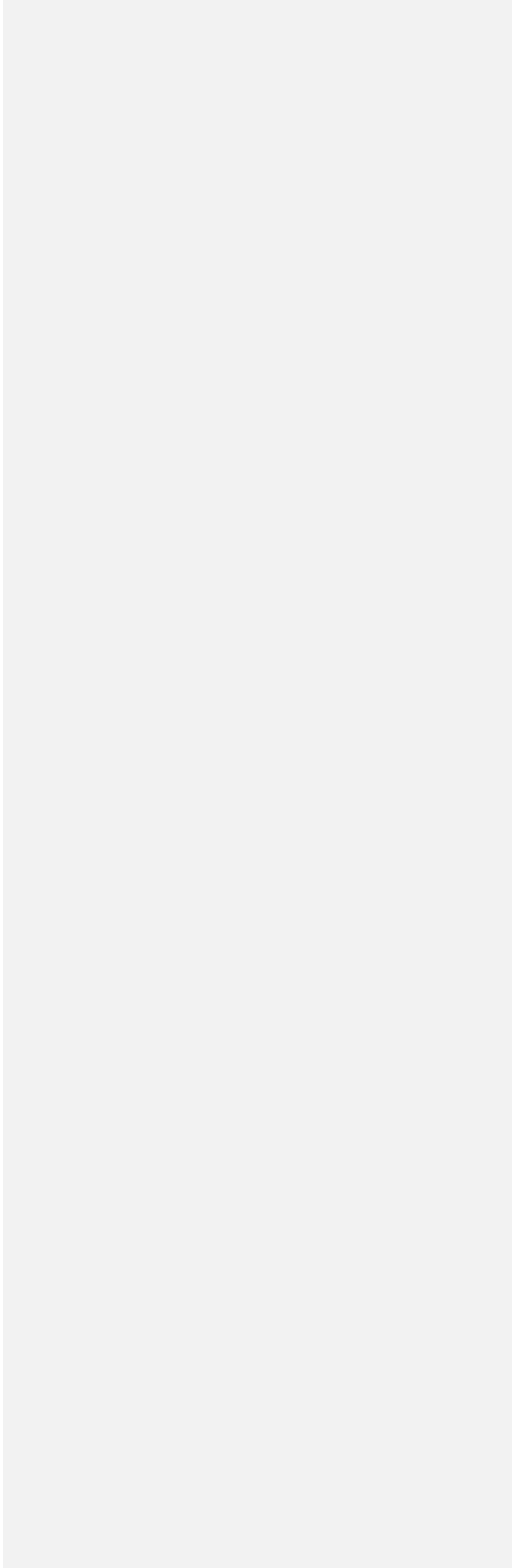
Roswell GA Police Department

Norcross GA Police Department

Duluth GA Police Department

Clarkston GA Police Department

8

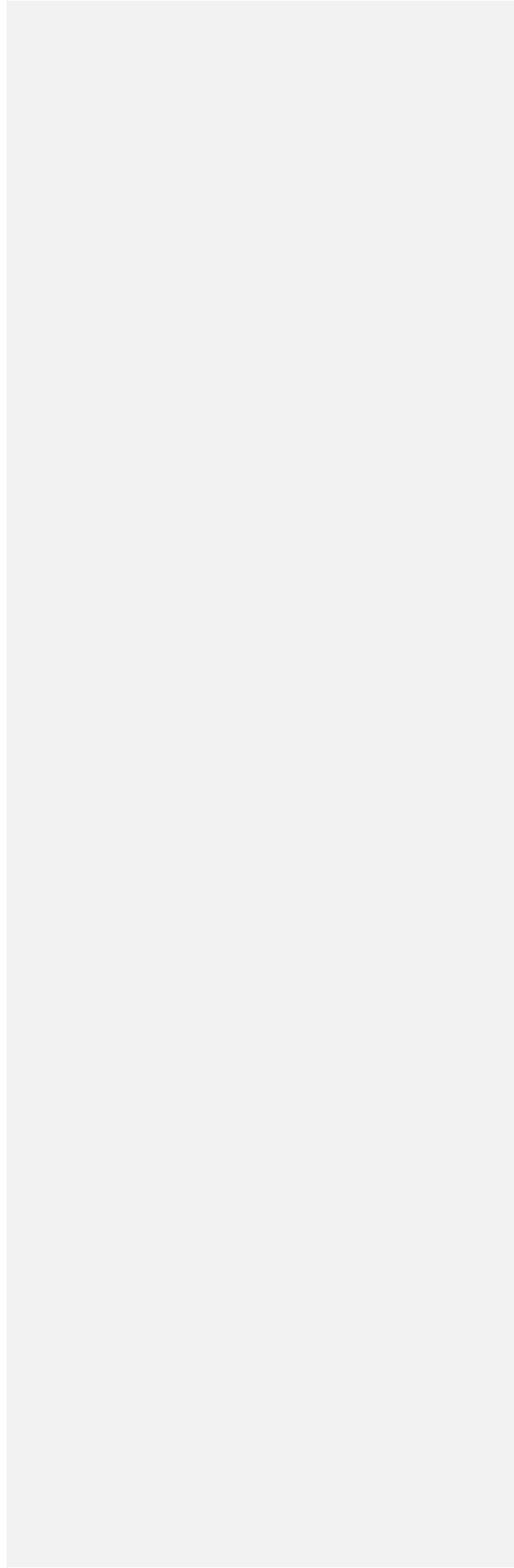


SCHEDULE 2**TECHNICAL AND ORGANISATIONAL MEASURES**

Flock has implemented the following technical and organisational measures (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

- 1) Organisational management and dedicated staff responsible for the development, implementation, and maintenance of Flock's information security program.
- 2) Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Flock's organisation, monitoring and maintaining compliance with Flock's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
- 3) Utilisation of commercially available and industry standard encryption technologies for Customer Personal Data that is:
 - a) being transmitted by Flock over public networks (i.e., the Internet) or when transmitted wirelessly; or
 - b) at rest or stored on portable or removable media (i.e., laptop computers, CD/DVD, USB drives, back-up tapes).
- 4) Data security controls which include at a minimum, but may not be limited to, logical segregation of data, logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).
- 5) Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Flock's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on Flock's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.
- 6) System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.
- 7) Physical and environmental security of data centre, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorised physical access, (ii) manage, monitor, and log movement of persons into and out of Flock facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.
- 8) Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Flock's possession.
- 9) Change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Flock's technology and information assets.
- 10) Incident / problem management procedures designed to allow Flock to investigate, respond to, mitigate, and notify of events related to Flock's technology and information assets.
- 11) Network security controls that provide for the use of firewall systems, intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
- 12) Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.
- 13) Business resiliency/continuity and disaster recovery procedures in an effort to maintain service and/or recovery from foreseeable emergency situations or disasters.

9



DocuSign Envelope ID: 39C4A31B-1980-4CBF-A6E9-4A6FEA0FB976

SCHEDULE 3

STANDARD CONTRACTUAL CLAUSES

For the purposes of the Standard Contractual Clauses:

1. Module Two shall apply in the case of the processing under clause 3.1(a)(i) of the DPA and Module Three shall apply in the case of processing under clause 3.1(a)(ii) of the DPA.
2. Clause 7 of the Standard Contractual Clauses (Docking Clause) does not apply.
3. Clause 9(a) Option 2 (General written authorization) is selected, and the time period to be specified is determined in clause 5.3 of the DPA.
4. The option in Clause 11(a) of the Standard Contractual Clauses (Independent dispute resolution body) does not apply.
5. For the Purpose of Annex I of the Standard Contractual Clauses, Schedule 1 contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority.
6. For the Purpose of Annex II of the Standard Contractual Clauses, Schedule 2 contains the technical and organisational measures.

7. The specifications for Annex III of the Standard Contractual Clauses, are determined by clause 5.1 of the DPA. The Sub-processor's contact person's name, position and contact details will be provided by Flock upon request.

SCHEDULE 4**ADDITIONAL SUPPLEMENTARY MEASURES**

Flock further commits to implementing supplementary measures based on guidance provided by EU supervisory authorities in order to enhance the protection of Customer Personal Data in relation to the processing in a third country, as described in this Schedule 4.

1. Additional Technical Measures (Encryption)

- 1.1 The personal data is transmitted (between the Parties and by Flock between data centers as well as to a Sub-processor and back) using strong encryption.
- 1.2 The personal data at rest is stored by Flock using strong encryption.

2. Additional Organisational Measures**1.3 Internal policies for governance of transfers especially with groups of enterprises**

- (a) Adoption of adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of formal or informal requests from public authorities to access the data.
- (b) Development of specific training procedures for personnel in charge of managing requests for access to personal data from public authorities, which should be periodically updated to reflect new legislative and jurisprudential developments in the third country and in the EEA.

1.4 Transparency and accountability measures

Regular publication of transparency reports or summaries regarding governmental requests for access to data and the kind of reply provided, insofar publication is allowed by local law.

1.5 Organisational methods and data minimization measures

Development and implementation of best practices by both Parties to appropriately and timely involve and provide access of information to their respective data protection officers, if existent, and to their legal and internal auditing services on matters related to international transfers of personal data transfers.

1.6 Others

Adoption and regular review by Flock of internal policies to assess the suitability of the implemented complementary measures and identify and implement additional or alternative solutions when necessary, to ensure that an essentially equivalent level of protection to that guaranteed within the EEA of the personal data transferred is maintained.

2. Additional Contractual Measures**2.1 Transparency obligations**

- (a) Flock declares that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data, (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require Flock to create or maintain back doors or to facilitate access to personal data or systems or for Flock to be in possession or to hand over the encryption key.

- (b) Flock will verify the validity of the information provided for the TIA questionnaire on a regular basis and provide notice to Customer in case of any changes without delay. Clause 14(e) of the SCCs shall remain unaffected.

DocuSign Envelope ID: 39C4A31B-1980-4CBF-A6E9-4A6FEA0FB976

2.2 Obligations to take specific actions

In case of any order to disclose or to grant access to the personal data, Flock commits to inform the requesting public authority of the incompatibility of the order with the safeguards contained in the Article 46 GDPR transfer tool and the resulting conflict of obligations for Flock.

2.3 Empowering data subjects to exercise their rights

- (a) Flock commits to fairly compensate the data subject for any material and non-material damage suffered because of the disclosure of his/her personal data transferred under the chosen transfer tool in violation of the commitments it contains.
- (b) Notwithstanding the foregoing, Flock shall have no obligation to indemnify the data subject to the extent the data subject has already received compensation for the same damage.
- (c) Compensation is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Flock's infringement of the GDPR.

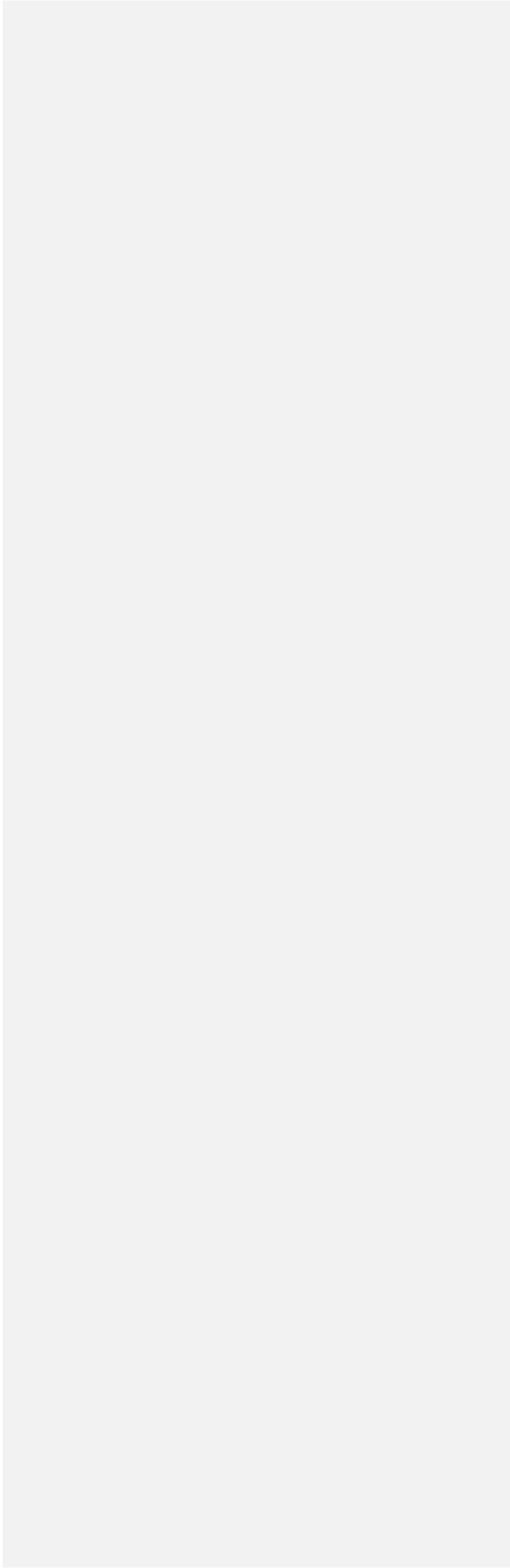
3. Additional obligations in case of requests or access by public authorities

2.4 Flock shall promptly inform Customer:

- (a) Of any legally binding requests from a law enforcement or other government authority ("**Public Authority**") to disclose the personal data shared by Customer ("**Transferred Personal Data**"); such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided. If permissible by law, Flock will make a good faith effort to provide the notification prior to the disclosure of any personal data in response to such requests.
- (b) If it becomes aware of any direct access by public authorities to transfer personal data in accordance with the laws of the country of destination, such notification shall include all information available to Flock.
- (c) If Flock is prohibited from notifying Customer and/or the data subject, Flock agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicate as much information and as soon as possible. Flock agrees to document its best efforts in order to be able to demonstrate them upon request of the data exporter.

2.5 Flock agrees to review, under the laws of the country of destination, the legality of the public authority's request, notably whether it remains within the powers granted to the requesting public authority and exhaust all available remedies to challenge the request if, after a careful assessment, Flock concludes that there are grounds under the laws of the country of destination to do so. This includes requests under section 702 of the United States Foreign Intelligence Surveillance Court ("**FISA**"). When challenging a request, Flock shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. Flock shall not disclose or provide access to the personal data requested until required to do so under the applicable procedural rules and, at such time, shall provide only the minimum amount of information required to comply with the request, based on a reasonable interpretation of the request.

12



SCHEDULE 5
UK AND SWISS ADDENDUM

1. UK ADDENDUM

With respect to any transfers of Customer Personal Data falling within the scope of the UK GDPR from Customer (as data exporter) to Flock (as data importer):

- 1.1 The Approved Addendum as further specified in this Schedule 5 shall form part of this DPA, and the Standard Contractual Clauses shall be read and interpreted in light of the provisions of the Approved Addendum, to the extent necessary according to Clause 12 of the Mandatory Clauses.
- 1.2 In deviation to Table 1 of the Approved Addendum and in accordance with Clause 16 of the Mandatory Clauses, the parties are further specified in Schedule 1 clause A of this DPA.
- 1.3 The selected Modules and Clauses to be determined according to Table 2 of the Approved Addendum are further specified in Schedule 3 of this DPA as amended by the Mandatory Clauses.
- 1.4 Annex 1 A and B of Table 3 to the Approved Addendum are specified by Schedule 1 of this DPA, Annex II of the Approved Addendum is further specified by Schedule 2 of this DPA, and Annex III of the Approved Addendum is further specified by Schedule 1 clause B.10 of this DPA.
- 1.5 Flock (as data importer) may end this DPA, to the extent the Approved Addendum applies, in accordance with clause 19 of the Mandatory Clauses.
- 1.6 Clause 16 of the Mandatory Clauses shall not apply.

2. SWISS ADDENDUM

As stipulated in clause 13 of the DPA, this Swiss Addendum shall apply to any processing of Customer Personal Data subject to Swiss data protection law or to both Swiss data protection law and the GDPR.

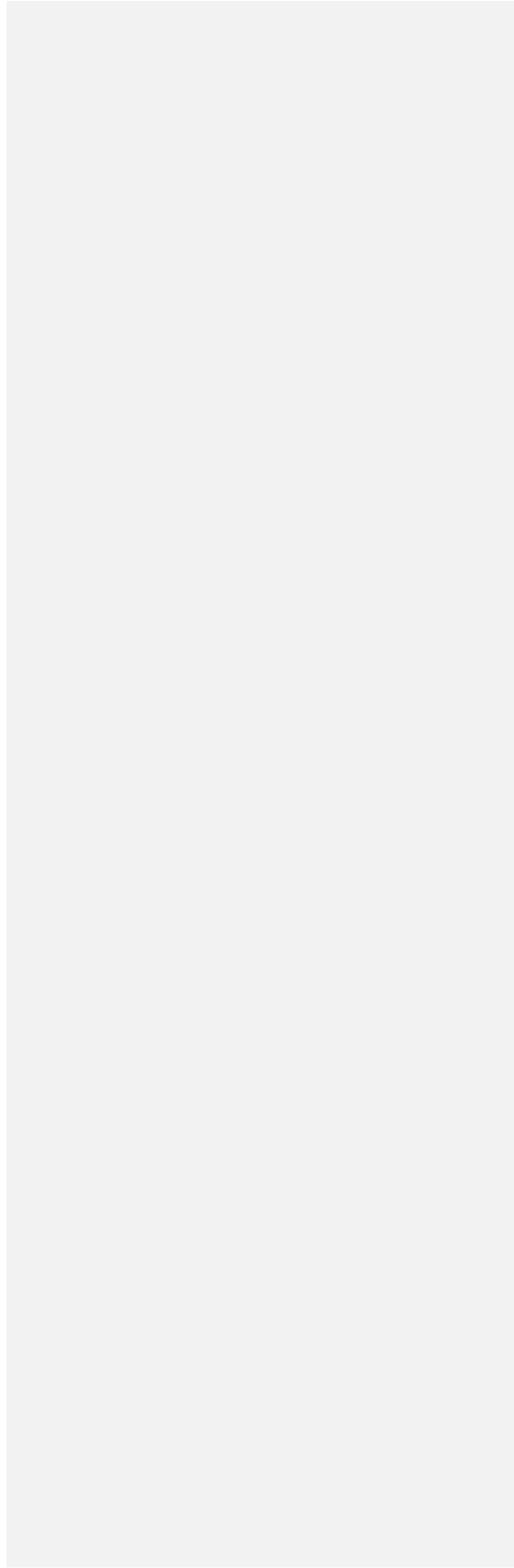
2.1 Interpretation of this Addendum

- (a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses as further specified in Schedule 3 of this DPA, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
Clauses	The Standard Contractual Clauses as further specified in Schedule 3 of this DPA
Swiss Data Protection Laws	The Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force from time to time.

- (b) This Addendum shall be read and interpreted in the light of the provisions of Swiss Data Protection Laws, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.
- (c) This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

- (d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.



Docusign Envelope ID: 39C4A31B-1980-4CBF-A6E9-4A6FEA0FB976

2.2 Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

2.3 Incorporation of the Clauses

(a) In relation to any processing of personal data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends the DPA including as further specified in Schedule 3 of this DPA to the extent necessary so they operate:

- (i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws or Swiss Data Protection Laws and the GDPR apply to the data exporter's processing when making that transfer; and
- (ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(b) To the extent that any processing of personal data is exclusively subject to Swiss Data Protection Laws, the amendments to the DPA including the SCCs, as further specified in Schedule 3 of this DPA and as required by clause 2.1 of this Swiss Addendum, include (without limitation):

- (i) References to the "Clauses" or the "SCCs" means this Swiss Addendum as it amends the SCCs.
- (ii) Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's processing when making that transfer."

- (iii) References to "Regulation (EU) 2016/679" or "that Regulation" or "GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.
- (iv) References to Regulation (EU) 2018/1725 are removed.
- (v) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".
- (vi) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner (the "FDPIC") insofar as the transfers are governed by Swiss Data Protection Laws;
- (vii) Clause 17 is replaced to state:
"These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by Swiss Data Protection Laws".
- (viii) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

Until the entry into force of the revised Swiss Data Protection Laws, the Clauses shall also protect personal data of legal entities and legal entities shall receive the same protection under the Clauses as natural persons.

- 2.4 To the extent that any processing of personal data is subject to both Swiss Data Protection Laws and the GDPR, the DPA including the Clauses as further specified in Schedule 3 of this DPA will apply (i) as is and (ii) additionally, to the extent that a transfer is subject to Swiss Data Protection Laws, as amended by

clauses 2.1 and 2.3 of this Swiss Addendum, with the sole exception that Clause 17 of the SCCs shall not be replaced as stipulated under clause 2.3(b)(vii) of this Swiss Addendum.

2.5

Customer warrants that it and/or Customer Affiliates have made any notifications to the FDPIC which are required under Swiss Data Protection Laws.