SOCKET MOBILE, INC.
Data Processing Addendum

This Socket Mobile, Inc. Data Processing Addendum ("**DPA**") reflects the parties' agreement with respect to the Processing of Personal Data by Socket Mobile, Inc. ("**Socket Mobile**") on behalf of the Customer in connection with the Socket Mobile Data Readers and Socket Mobile Software and Data related Terms of Use and Conditions (collectively referred to in this DPA as the "**Applications**"). The term of this DPA shall follow the term of the Applications.

This DPA applies where and only to the extent that Socket Mobile processes Personal Data on behalf of the Customer in the course of providing the Services and such Personal Data is subject to Data Protection Laws of the appropriate jurisdiction, including the State of California, Japan, Ireland, the European Union, the European Economic Area and/or its member states, Switzerland and/or the United Kingdom. The parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

Socket Mobile updates these terms from time to time and will notify the Customer via in-app and email notifications.

1. Definitions

The following terms have the meanings set forth below.

- **"Affiliate"** means any entity, whether incorporated or not, which is controlled by or under common control, either directly or indirectly, with a party to this DPA.
- "**Business**," "**Sell**," "**Service Provider**," and "**Third Party**" all have the definitions given to them in the CCPA.
- **"Customer"** means the end user customer that purchased the Services under the Applications.
- "**Data Controller**" or **"Controller"** means the entity that determines the purposes and means of the Processing of Personal Data. Data Controller includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Business" or "Third Party," as context requires.
- **"Data Protection Law"** means all data protection and privacy laws applicable to the processing of Personal Data under the Applications as it relates to the Customer, including Regulation 2016/679 (General Data Protection Regulation) ("**GDPR**"), and Cal. Civ. Code Title 1.81.5, § 1798.100 et seq. (California Consumer Privacy Act) ("**CCPA**").
- **"Data Subject"** means an identified or identifiable natural person.
- **"EEA"** means the European Economic Area.
- **"Personal Data"** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Personal Information," as context requires.
- **"Personal Data Breach"** means a breach of security of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.
- **"Process"** or **"Processing"** means any operation or set of operations which is performed upon Personal Data, whether by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- **"Data Processor"** means an entity that processes Personal Data on behalf of another entity. Data Processor includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Service Provider," as context requires.

- **"Sensitive Data"** means the following types and categories of data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data; data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; data concerning a natural person's sex life or sexual orientation; government identification numbers (e.g., SSNs, driver's license); payment card information; nonpublic personal information governed by the Gramm Leach Bliley Act; an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; and precise geolocation.
- "**Service"**, **"Services"**, or **Service Offering"** means the Socket Mobile Data Readers and Socket Mobile Software and Data related Terms of Use and Conditions provided under the Applications and this DPA.
- **"Standard Contractual Clauses"** means the clauses attached hereto as **Annex 1**, set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of Data Protection, as well as any modified clauses, described in the UK Addendum, attached here as **Annex 2**, set out by the United Kingdom pursuant to UK GDPR, the UK Data Protection Act 2018 and the UK Privacy and Electronic Communications Regulations 2003.
- **"Sub-processor"** means a third-party processor engaged by the Processor who has or will have access to or process Personal Data from the Data Controller.
- **"You"** means the Data Controller.

2. Rights and Obligations of the Data Controller.

2.1. Within the scope of the DPA and in its use of the Services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. For the avoidance of doubt, Controller's instructions for the Processing of Personal Data shall comply with the Data Protection Law. This DPA contains Controller's complete and final instructions to Socket Mobile in relation to Personal Data. Any additional instructions outside the scope of this DPA require prior written agreement signed by both parties.

2.2. Controller's initial instructions to the Data Processor regarding the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data, and categories of Data Subjects are set forth in this DPA and **Appendix 1** ("**Instructions**").

2.3. Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

2.4. Notification(s) of information concerning the Processing or Personal Data Breach will be delivered to the Data Controller's registered notification email address. It is Controller's sole responsibility to ensure that it maintains accurate contact information with Socket Mobile at all times.

2.5. If claims are placed on one of the contracting parties by a Data Subject in connection with any claim as per Art. 82 of the GDPR, the contracting party concerned shall notify the other party without undue delay. The contracting parties shall support one another in defending the claim.

3. Obligations of the Processor;

3.1. Compliance with Instructions.

3.1.1. You acknowledge and agree that you are the Controller of Personal Data and Socket Mobile is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's Instructions. If the Processor believes that any of the

Instructions of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under any Data Protection Law, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Controller under the Agreement for any failure to perform the applicable services until such time as the Controller issues new instructions in regard to the Processing.

3.1.2. The Data Processor shall produce and update a list of all categories of activities which it carries out on behalf of the Data Controller, including the compulsory specifications according to Art. 30 para. 2 of the GDPR as set out in **Appendix 1.**

3.1.3. The Data Processor shall appoint the contact partner for Controller for data protection questions arising within the framework of the Agreement and this DPA as set forth in **Appendix 1**.

3.2. **Security.** The Data Processor will implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under **Appendix 2** to this DPA ("**Security Measures**"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

3.3. **Compliance.** The Data Processor is not responsible for compliance with any Data Protection Laws applicable to the Data Controller's industry that are not generally applicable to the Data Processor. The Data Processor shall not be required to provide or disclose information that would violate applicable law, a duty of confidentiality, or any other obligation owed to a third party.

3.4. **Data Breaches.** The Data Processor shall notify the Data Controller without undue delay if the Data Processor becomes aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

3.5. **Confidentiality.** The Data Processor shall ensure that any personnel whom the Data Processor authorizes to process Personal Data on its behalf is subject to appropriate confidentiality obligations with respect to that Personal Data.

3.6. **Sub-Processors.** The Data Processor may engage Sub-Processors to Process Personal Data on behalf of the Data Controller. Socket Mobile has currently appointed, as Sub-Processors, the third parties listed in **Appendix 2** to this DPA. The Data Processor will notify the Data Controller if the Data Processor adds or replaces any Sub-Processors listed in **Appendix 3** at least 30 days prior to any such changes via the Socket Mobile Cloud portal. Where Sub-Processors are utilized, Socket Mobile will impose data protection terms on the Sub-Processors that will require at least the same level of protection for Personal Data as those in this DPA to the extent applicable to the nature of the services provided by the Sub-Processor.

3.7. **Data Transfers.** You acknowledge and agree that Socket Mobile may process Personal Data on a global basis as necessary to provide the Service in accordance with the Agreement, and in particular

that Personal Data may be transferred to and processed by Socket Mobile in the United States and to other jurisdictions where Socket Mobile Affiliates and Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each Party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

Where applicable, the Standard Contractual Clauses at **Annex 1** will apply with respect to Personal Data that is transferred outside the EEA to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the Data Protection Law), with the exception of Personal Data that is transferred outside the UK, which is governed by the UK Addendum, attached hereto as **Annex 2**.

4. Additional Provisions for European Data.

4.1. Scope: This 'Additional Provisions for European Data' section shall apply only with respect to European Data.

4.2. Roles of the Parties: When Processing European Data in accordance with the Instructions, the Parties acknowledge and agree that you are the Controller of European Data, and we are the Processor.

4.3. Objection to New Sub-Processors: Socket Mobile will give Data Controller the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Personal Data within 30 days of notifying you in accordance with the 'Sub-Processors' section of this DPA. If you do notify us of such an objection, the Parties agree to discuss Data Controller's concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the Service in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination). The Parties agree that by complying with this section, Socket Mobile fulfills its obligations under Section 9 of the Standard Contractual Clauses.

4.4. Sub-Processor Agreements: For the purposes of Clause 9(c) of the Standard Contractual Clauses, the Customer acknowledges that Socket Mobile may be restricted from disclosing Sub-Processor agreements but shall use reasonable efforts to require any Sub-Processor appointed to permit it to disclose the Sub-Processor agreement to you and shall provide (on a confidential basis) all information we reasonably can.

4.5. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws.

4.6. Transfer Mechanisms for Data Transfers: Socket Mobile shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance

with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

4.7. The Customer acknowledges that in connection with the performance of the Services, Socket Mobile is a recipient of European Data in the United States. The Parties acknowledge and agree as follows:

4.7.1. **Standard Contractual Clauses**: The Parties agree to abide by and process European Data in compliance with the Standard Contractual Clauses, as populated in **Annex 1**.

4.7.2. The Parties agree that for the purposes of the Standard Contractual Clauses, (i) Socket Mobile, will be the "data importer" and Customer will be the "data exporter" (on behalf of itself and Permitted Affiliates); (ii) the Annexes of the Standard Contractual Clauses shall be populated with the relevant information set out in **Appendix 1** and **Appendix 2** of this DPA; (iii) where the Socket Mobile contracting entity under the Agreement is not Socket Mobile, such contracting entity (not Socket Mobile) will remain fully and solely responsible and liable to you for the performance of the Standard Contractual Clauses by Socket Mobile, and you will direct any instructions, claims or enquiries in relation to the Standard Contractual Clauses to such contracting entity; and (iv) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

4.7.3. To extent that and for so long as the Standard Contractual Clauses as implemented in accordance with this DPA cannot be relied on by the parties to lawfully transfer Personal Data in compliance with the UK GDPR, the applicable standard data protection clauses issued, adopted or permitted under the UK GDPR shall be incorporated by reference, and the annexes, appendices or tables of such clauses shall be deemed populated with the relevant information set out in **Appendix 1** and **Appendix 2** of this DPA.

4.7.4. If for any reason Socket Mobile cannot comply with its obligations under the Standard Contractual Clauses or is breach of any warranties under the Standard Contractual Clauses, and the Customer intends to suspend the transfer of European Data to Socket Mobile or terminate the Standard Contractual Clauses, the Customer agrees to provide Socket Mobile with reasonable notice to enable Socket Mobile to cure such non-compliance and reasonably cooperate to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If Socket Mobile cannot cure the non-compliance, the Customer may suspend or terminate the affected part of the Service in accordance with the Agreement without liability to either Party (but without prejudice to any fees that have been incurred prior to such suspension or termination).

4.8. **Demonstration of Compliance:** Processor shall make all information reasonably necessary to demonstrate compliance with this DPA available to Controller and allow for and contribute to audits, including inspections conducted by or your auditor in order to assess compliance with this DPA. You acknowledge and agree that you will exercise your audit rights under this DPA and Clause 8.9 of the Standard Contractual Clauses by instructing us to comply with the audit measures described in this ‘Documentation and Compliance' section. You acknowledge that Socket Mobile Cloud is hosted by our data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are regularly tested by independent third-party penetration testing firms. Upon your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you

necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year, unless you have reasonable grounds to suspect non-compliance with the DPA.

5. Additional Provisions for California Personal Information.

5.1. Scope: This 'Additional Provisions for California Personal Information' section of this DPA will apply only with respect to California Personal Information.

5.2. Roles of the Parties: When processing California Personal Information in accordance with your Instructions, the Parties acknowledge and agree that you are a Business, and we are a Service Provider for the purposes of the CCPA

5.3. Responsibilities: The Parties agree that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services under the Agreement (the "**Business Purpose**") or as otherwise permitted by the CCPA.

Appendix 1: Data Processing Details

The following Instructions apply to the Processing of the Personal Data under this DPA:

Data Exporter
Name: The Customer, as defined herein.
Address: The Customer's address, as provided by Customer or by Socket Mobile's authorized reseller.
Customer Contact (person's name, position and contact details): The Customer's contact details, as set out in the Agreement and/or as set out in Customer's Socket Mobile Cloud Account.
Activities Relevant to the Data Transferred Under these Clauses: Processing of Personal Data in connection with Customer's use of the Services under the Agreement.
Role: Controller.

Data Importer
Name: Socket Mobile, Inc.
Address: 40675 Encyclopedia Circle, Fremont, CA 94538.
Contact Person's Name: Len Ott, len@socketmobile.com.
Activities Relevant to the Data Transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the under the Agreement.

Processing Operations and Purposes
The Processing shall include the following operations and purposes:

- Storage and forwarding of data and other processing necessary to provide, maintain, and improve the Service provided to the Data Controller;
- To provide technical support to the Data Controller; and
- Disclosures in accordance with the DPA, as compelled by law

Categories of Data
The Personal Data Processed might include the following categories of Data:

- First and last name
- Employer
- Contact information (company, email, phone, business address)
- IP Information
- Location data
- User interactions with the Service

Categories of Data Subjects
The Personal Data Processed might include the following categories of Data Subjects:

- Data Controller's business management and employees
- Customers

Retention Period
The Personal Data shall be erased at the Data Controller's request according to the Data Controller's Instructions. If the Data Processor is unable to delete Personal Data for technical or other reasons, the Data Processor will apply measures to ensure that Personal Data is blocked from any further processing.

Appendix 2: Security Measures

Processor agrees to implement the following Security Measures to protect Personal Data:

Access Control

1. Preventing Unauthorized Product Access.

a. Outsourced processing: The Service is hosted with outsourced cloud infrastructure providers. Contractual agreements, privacy policies, and vendor compliance programs are in place to protect data processed or stored by these vendors.

b. Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

c. Authorization: Customer data is accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model ensures that only the appropriately assigned individuals can access relevant features, views, and customization options.

2. Preventing Unauthorized Product Use. We implement industry standard access controls and detection capabilities for the internal networks that support its products.

a. Access Controls**:** Network access control mechanisms are in use to prevent network traffic using unauthorized protocols from reaching the product infrastructure. These technical measures include security group assignment, and traditional firewall rules.

b. Intrusion Detection and Prevention**:** We implement a Web Application Firewall (WAF) solution.

c. Static Code Analysis**:** We perform security reviews of code as part of our deployment process.

d. Penetration Testing**:** We employ penetration tests annually and upon significant change.

e. Product Access**:** A subset of our employees have access to our Services in order to provide effective customer support, troubleshoot potential problems, and detect and respond to security incidents and implement data security. Employees are granted access by role and access is reviewed bi-annually.

f. Transmission Control:

i. In-transit: HTTPS encryption (also referred to as SSL or TLS) is required on all interfaces. Our HTTPS implementation uses industry standard algorithms and certificates.
ii. At-rest: User passwords are stored following policies that follow industry standard practices for security. Stored data is encrypted at rest.

g. **Availability Control.** Measures are in place to ensure that Personal Data are protected from accidental destruction or loss, including:
    i. infrastructure redundancy;
    ii. backups stored at an alternative site and available for restore in case of failure of the primary system.

h. **Input Control.**
    i. Detection: All system behavior, traffic received, system authentication, and other application requests are logged. Internal systems aggregate and correlate log data and alert appropriate employees of malicious, unintended, or anomalous activities.

    ii. Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

    iii. Session time-outs are in place for sessions that have been idle for an identified period of time and lock-outs are in place for excessive invalid login attempts.

Sub -Processor	Purpose	Applicable Service	Address	Data Protection and Privacy Information
Microsft Azure	Hosting & Infrastructure	Cloud computing platform	One Microsoft Way, Redmond, Washington, United States	https://www.microsoft.com/en-gb/privacy/privacystatement
Micrososft Dynamics365	CRM	CRM	One Microsoft Way, Redmond, Washington, United States	https://www.microsoft.com/en-gb/privacy/privacystatement
RingCentral	Telephony, Video, SMS communications	Cloud based communications	20 Davis Dr, Belmont, United States	https://www.ringcentral.com/legal/last-update-july-29-2024/privacy-notice.html
Survey Monkey	Customer feedback	Online survey	101 Lytton Avenue, Palo Alto, California 94301, United States	https://www.surveymonkey.com/mp/legal/privacy/
Google Analytics	Capture of website usage data	Search engine optimization and usage analysis	1600 Amphitheatre Parkway, Moutain View, CA 94043, USA	https://support.google.com/analytics/answer/7318509?hl=en
Shopify	Webstore hosting	E-commerce webstore	151 O'Connor Street, Ground floor, Ottawa, Canada,	https://www.shopify.com/legal/privacy
PayPal	Online payments in webshops	Payment processing platform	2211 North First Street, San Jose, CA 95131, United States	https://www.paypal.com/uk/legalhub/paypal/privacy-full
Stripe	Online payment processing	Payment processing platform	354 Oyster Point Blvd, South San Francisco, United States.	https://stripe.com/gb/privacy
Twilio SendGrid	Customer notifications	Email marketing campaign tool	101 Spear Street, Fifth Floor HQ, San Francisco, United States	https://www.twilio.com/en-us/legal/privacy
Click Dimensions	Email Marketing and Campaign Automation	Email marketing campaign tool	5901 Peachtree Dunwoody Road, NE Suite B500, United States	https://clickdimensions.com/solutions-security-and-privacy/
Ezi Returns	Global RMA processing	Returns processing hubs	The Oaks, Calverhall, Whitchurch, Shropshire, SY13 4PE, United Kingdom	https://www.ezireturns.com/privacy-policy
iPacky	Order fulfilment system	Order fulfilment and serial number processing	Fossveien 72, 1405 Langhus, Norway	https://ipacky.com/privacy-policy/
Refersion	Affiliate program	Affiliate marketing program tool	242 W 38th St., New York, NY 10018, United States	https://www.refersion.com/privacy/
Flow	Process automation	Low code custom proces automations	151 O'Connor Street, Ground floor, Ottawa, Canada,	https://www.shopify.com/legal/privacy
Kalx Follow - Up	Automated follow up email marketing	Email Marketing	110 Hamilton Ave, 110A, Columbus, OH, 43203, US	https://www.followupemailapp.com/privacy-policy
Klaviyo	Webstore email notifications	Marketing automation platform	125 Summer St Floor 6, Boston, United States	https://www.klaviyo.com/legal/privacy
Langify	Webshop language translation	Localized translations	Im Robbenklee 29a, Herford, 32052, DE	https://langify-app.com/privacy_policy
Metafields Guru	Custom webshop storefront design	Storefront design	Lystopadova street, 5, Ternopil, 46000, UA	https://metafields.guru/Metafields_Guru_Privacy_Policy.pdf
MyBulk Discounts Creator	Customized bulk discount creation tool	Bulk discount creator	9 POUND LANE, GODALMING, ENG, GU7 1BX, GB	https://spacesquirrel.co/privacy-policy
Order Printer	Sending webstore invoices to customers	Custom invoice creator	151 O'Connor Street, Ground floor, Ottawa, Canada,	https://www.shopify.com/legal/privacy
WOD: Pre-Order Now	Pre-order supply management	Pre-order stock management and out-of-stock control	729 Hymettus Ave, Encinitas, CA, 92024, US	https://websiteondemand.ca/pre-order-now-privacy-policy/
Report Pundit	Used to analyze webstore data	Report generate for webstore data	409 Yellowtail Road, Libby, MT, 59923, US	https://www.reportpundit.com/privacy-policy
Sufio: Professional Invoices	Automate VAT validation for EU orders. Generate invoices and create credit notes.	Generate invoices and manage VAT validation	Bottova 1, Bratislava, 81109, SK	https://sufio.com/legal/privacy-policy/

Annex 1

The parties agree that the following Standard Contractual Clauses - as updated by the EU in June 2021 - shall apply as to all transfers of personal data to countries outside the EEA without an adequacy decision.

Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "**data exporter**"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "**data importer**") have agreed to these standard contractual clauses (hereinafter: "**Clauses**").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9 - Clause 9(a), (c), (d) and (e);
(iv) Clause 12 - Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);
(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation
(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy
In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)
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 specified in Annex I.B.

Clause 7
Docking clause
(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards
The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions
(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation
The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency
On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy
If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data
Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter "**personal data breach**"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "**sensitive data**"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "**onward transfer**") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors
(a) The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights
(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress
(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability
(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision
(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses
(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorizing access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification
(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV - FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law
These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that these Clauses shall be governed in accordance with the 'Contracting Entity; Applicable Law; Notice' section of the Jurisdiction Specific Terms or if such section does not specify an EU Member State, by the law of the Republic of Ireland (without reference to conflicts of law principles).

Clause 18
Choice of forum and jurisdiction
(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the jurisdiction specified in Clause 17.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex 2

UK AND SWISS ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

(a) This Addendum amends the Standard Contractual Clauses to the extent necessary, so they operate for transfers made by the data exporter to the data importer, to the extent that the UK GDPR or Swiss DPA (as defined in the Socket Mobile Data Processing Addendum) apply to the data exporter's processing when making that transfer.

(b) The Standard Contractual Clauses shall be amended with the following modifications:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR or Swiss DPA (as applicable);

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the UK GDPR or Swiss DPA (as applicable);

(iii) references to Regulation (EU) 2018/1725 shall be removed;

(iv) references to "EU", "Union" and "Member State" shall be replaced with references to the "UK" or "Switzerland" (as applicable);

(v) Clause 13(a) and Part C of Annex II are not used and the "competent supervisory authority" shall be the United Kingdom Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);

(vii) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and

(viii) to the extent the UK GDPR applies to the processing, Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts"; and

(ix) to the extent the Swiss DPA applies to the processing, Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts".