THEDATASAFE

DATA PRIVACY & DATA SECURITY ADDENDUM

Exhibit to THEDATASAFE Terms and Conditions

This Data Privacy & Data Security Addendum (the "Addendum") is an Addendum to THEDATASAFE Terms and Conditions (the "TC"). This Addendum governs the Parties' obligations with regard to the privacy and security of Customer Data. Any capitalized term not otherwise defined in this Addendum shall have the meaning given to it in the TC.

DEFINITIONS

"**Authorized Persons**" means THEDATASAFE employees, agents, and contractors that have a need to know or otherwise access Customer Data to enable THEDATASAFE to perform the Services.

"**Controller**" means a controller as defined under the General Data Protection Regulation (GDPR).

"**Customer Data**" means all data relating to Customer that is (i) provided to THEDATASAFE by or on behalf of Customer or (ii) otherwise obtained, accessed, developed, or produced by THEDATASAFE. Customer Data includes Personal Data.

"**Data Protection Laws**" means all international, federal, national and state privacy and data protection laws and regulations to the extent applicable to THEDATASAFE and the Services.

"**Data Breach**" means any loss or unauthorized access, acquisition, theft, destruction, disclosure or use of Customer Data that occurs while such Customer Data is in the possession of or under the control of THEDATASAFE.

"**GDPR**" means the EU General Data Protection Regulation 2016/679.

"**Parties**" means Customer and THEDATASAFE.

"**Personal Data**" means information relating to an identified or identifiable natural person (the "**Data Subject**"). An identifiable natural person is a natural person who can be identified, directly or indirectly, 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.

"**Process**" or "**Processing**" means any operation or set of operations that are performed upon Customer Data, whether or not by automatic means, such as collection, accessing, processing, use, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, transmittal, alignment or combination, blocking, erasure, destruction or otherwise used as set out in the applicable Data Protection Laws.

"**Processor**" means a processor as defined under the GDPR.

"**Services**" means the services, products and other activities to be provided to or carried out by or on behalf of THEDATASAFE for Customer pursuant to the TC.
"**Sub-Processor**" shall mean an entity engaged by THEDATASAFE to assist it in Processing the Customer Data in fulfilment of its obligations under the TC.

"**Third Party**" is any person or entity other than THEDATASAFE and Customer.

DATA PRIVACY

1. Compliance with Laws: The Parties shall comply with their obligations under all Data Protection Laws. For purposes of the GDPR, Customer is considered the Controller and THEDATASAFE is its Processor. If Customer is considered a Processor for purposes of the GDPR, then THEDATASAFE is considered its Sub-Processor.

2. Distribution of Customer Data: Customer shall only provide THEDATASAFE with Personal Data that is needed by THEDATASAFE to provide the Services to Customer. THEDATASAFE shall not be responsible for any additional Personal Data. Customer represents and warrants that it has obtained all consents from any Controller or Data Subject necessary to provide the Personal Data that it makes available to THEDATASAFE pursuant to this Addendum.

3. Limitations on Use of Personal Data: THEDATASAFE shall not Process Customer Data other than for the purposes specified by Customer. THEDATASAFE shall not Process Customer Data for the benefit of any Third Party. THEDATASAFE shall access only the Customer Data that it needs to perform the Services (i.e., no more than necessary). THEDATASAFE will not store Customer Data longer than necessary to achieve the permitted purposes specified by Customer.

4. Restrictions: Except with Customer's prior, written approval, on a case-by-case basis, THEDATASAFE will not: (a) use Customer Data other than as necessary for THEDATASAFE to provide the Services and its obligations under this Addendum, (b) disclose, sell, assign, lease or otherwise provide Customer Data to Third Parties (other than to its affiliates or Sub-Processors), except to Data Subjects to the extent required or permitted by Data Protection Laws, or (c) merge Customer Data with other data, modify or commercially exploit any Customer Data.

5. Sensitive Personal Data: In no event will Customer provide any Sensitive Personal Data to THEDATASAFE unless it is protected through use of hashing, encryption, authentication or other protective controls. "Sensitive Personal Data" is defined as (a) information that reveals a natural person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, (b) information or data concerning a natural person's health or sex life or sexual orientation; or (c) genetic data or biometric data about a natural person.

SUB-PROCESSORS

THEDATASAFE may engage Sub-Processors in connection with the provision of the Services, provided, however, that THEDATASAFE may not provide a Sub-Processor with access to Customer Data unless the Sub-Processor has: (i) a business need to know / access the relevant Customer Data, as necessary for the purposes of the Services or the TC; and (ii) signed a written obligation of confidentiality or are under professional obligations of confidentiality. Upon Customer's request, THEDATASAFE shall provide Customer with a list of Sub-Processors.

THEDATASAFE

DATA SUBJECT RIGHTS AND COOPERATION

THEDATASAFE shall use commercially reasonable efforts to cooperate and assist with a Data Subject's exercise of his/her rights under applicable Data Protection Laws with respect to Personal Data Processed by THEDATASAFE, including, without limitation, the right to be forgotten, the right to data portability, and the right to access data under the GDPR. THEDATASAFE shall promptly notify Customer if THEDATASAFE receives any such request.

RETURN OR DESTRUCTION OF CUSTOMER DATA

Upon the written request of Customer, THEDATASAFE will return a copy of all Customer Data to Customer in a commonly readable format or securely delete Customer Data as soon as reasonably practicable and subject to THEDATASAFE customary backup procedures. However, if THEDATASAFE is required by law to retain Customer Data or if Customer Data is stored in a manner such that it cannot readily be returned or destroyed without affecting other data, then THEDATASAFE will continue to protect such Customer Data in accordance with this Addendum and limit any use to the purposes of such retention.

DATA SECURITY

1. Security Program Requirements: THEDATASAFE will maintain a security program that contains administrative, technical, and physical safeguards appropriate to the complexity, nature, and scope of its activities. THEDATASAFE security program shall be designed to protect the security and confidentiality of Customer Data against unlawful or accidental access to, or unauthorized processing, disclosure, destruction, damage or loss of Customer Data. At a minimum, THEDATASAFE security program shall include: (a) limiting access of Customer Data to Authorized Persons; (b) managing authentication and access controls of the system components that provide the services, back-up systems, operating systems, storage media and computing equipment (excluding Bring Your Own Device (BYOD) equipment of personnel of Customer, its Affiliates or its contractors); (c) implementing network, application, database, and platform security; (d) means for securing information transmission, storage, and disposal within THEDATASAFE possession or control; (e) means for encrypting Customer Data stored on media within THEDATASAFE possession or control by using modern acceptable cyphers and key lengths, including backup media; (f) means for encrypting Customer Data transmitted by THEDATASAFE over public or wireless networks by using modern acceptable cyphers and key lengths; and (g) means for keeping firewalls, routers, servers, personal computers, and all other resources current with appropriate security-specific system patches.

2. Regular Reviews: THEDATASAFE shall ensure that its security measures are regularly reviewed and revised to address evolving threats and vulnerabilities.

DATA BREACH PROCEDURES

Notification: THEDATASAFE shall notify Customer of any Data Breach as soon as practicable and without undue delay after becoming aware of it. Such notification shall at a minimum: (i) describe the nature of the Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned; (ii) communicate the name and contact details of THEDATASAFE data protection officer or other relevant contact from whom

more information may be obtained; and (iii) describe the measures taken or proposed to be taken to address the Data Breach.

Remedial Actions: In the event of a Data Breach caused by THEDATASAFE, THEDATASAFE will use commercially reasonable efforts to: (a) remedy the Data Breach condition, investigate, document, restore Customer service(s), and undertake required response activities; (b) provide regular status reports to Customer on Data Breach response activities; (c) assist Customer with the coordination of media, law enforcement, or other Data Breach notifications; and (d) assist and cooperate with Customer in its Data Breach response efforts.

CROSS-BORDER TRANSFERS

Location: THEDATASAFE systems and THEDATASAFE Processing of Customer Data will occur only within Switzerland (the "Processing Jurisdiction"). THEDATASAFE will not transfer any Customer Data outside of the Processing Jurisdiction without the prior written agreement of Customer.

Sub-Processors: THEDATASAFE will use commercially reasonable efforts to ensure that Sub-Processors will either be certified under the EU-US Privacy Shield or that the Sub-Processors execute EU-prescribed Standard Contractual Clauses.

INDEMNIFICATION

Each Party ("Indemnifying Party") shall defend, indemnify, and hold harmless the other Party and its subsidiaries, affiliates, and their respective officers, directors, employees, agents, successors, and permitted assigns ("Indemnified Parties") from and against all losses, damages, liabilities, actions, judgments, penalties, fines, costs, or expenses (including reasonable attorneys' fees) arising from any Third-Party claims against any such Indemnifying Parties (collectively, "Losses") to the extent such Losses result from (i) a Data Breach caused by the Indemnifying Party; or (ii) the Indemnifying Party's failure to materially comply with any of its obligations under this Addendum. The Indemnifying Party's obligations are subject to the Indemnified Party: (a) promptly notifying the Indemnifying Party of the claim giving rise to the indemnity; (b) providing the Indemnifying Party with sole control and authority over the defense of such claim and all related settlement negotiations; and (c) providing the Indemnifying Party, at the Indemnifying Party's request and expense, with all information and assistance reasonably necessary or useful by the Indemnifying Party to defend and/or settle any such claim or action.

AUDITS REPORTS

Without limiting any of THEDATASAFE other obligations under this Article, if THEDATASAFE engages a third-party auditor to perform a data security audit of THEDATASAFE operations, information security program or disaster recovery/business continuity plan, THEDATASAFE, at Customer's written request, shall provide a copy of the audit report to Customer. Any such audit reports shall be THEDATASAFE confidential information.

LIMIT ON LIABILITY

Notwithstanding anything to the contrary in this Addendum or the TC, each Party's liability to the other hereunder is subject to the limitations set forth in the TC. This Section shall not be construed as limiting the liability of either Party with respect to claims brought by Data Subjects.

REMEDIES

Each Party acknowledges that any breach of its covenants or obligations set forth in this Addendum may cause the other Party irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the other Party is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance, and any other relief that may be available from any court, in addition to any other remedy to which it may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum or the TC to the contrary.

MISCELLANEOUS

Conflicts: In the event of any conflict or inconsistency between the provisions of this Addendum and the provisions of the TC, the provisions of this Addendum shall prevail.

Governing Law: This Addendum shall be governed by and construed in accordance with the choice of law in the TC.