DATA PROTECTION ADDENDUM

This Data Protection Addendum ("DPA") forms part of the Service Terms and Conditions found at https://duo.com/legal/terms, unless Customer has entered into a written agreement, in which case, this DPA form part of such written agreement.

How to Execute This DPA:

1. This DPA consists of several parts: (a) the main body of the DPA, (b) Annex A, and (c) Annex B,, the Standard Contractual Clauses (including Appendices 1, 2 and 3).
2. This DPA has been pre-signed on behalf of Duo Security. The Standard Contractual Clauses in Annex B have been pre-signed by Duo Security, as the data importer.
3. To complete this DPA, Customer must:
    a. Complete the information in the signature box and sign on page 9.
        i. Ensure Customer's name is as it appears on a valid Duo Security Order Form, Service Terms and Conditions ("Agreement") or Admin Panel.
    b. Complete the information as the data exporter on page 21.
    c. Complete the information in the signature box and sign on page 32
4. Once you have completed and signed the DPA per the steps above, submit this to Duo Security by returning this by email to GDPR@duo.com.

Upon receipt of a validly completed DPA by Duo Security at this email address, this DPA will become legally binding. If the organization signing this DPA is neither a party to an Order Form nor an Agreement, this DPA is not valid and is not legally binding. In order to demonstrate to relevant supervisory authorities that we are holding ourselves to the same standards across all customers and that privacy is embedded into our organization, we are using this standard DPA consistently with all customers and do not entertain edits. If you have any questions on this matter, please reach out to our team at GDPR@duo.com.

DATA PROTECTION ADDENDUM

This Data Processing Addendum ("**DPA**"), effective as of 25 May 2018 or, if after 25 May 2018, the date of the final signatures, forms part of the Agreement between Customer on behalf of itself and to the extent required under the Data Protection Laws (as defined below), on behalf of its Controller Affiliate(s) (as defined below) and Duo Security, Inc. ("**Duo Security**") and applies where, and to the extent that, Duo Security processes Personal Data on behalf of Customer when providing Services under the Agreement. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. The data processing agreement and / or model clause agreement, if any, previously entered into by Duo Security and Customer shall be superseded and replaced with this DPA.

1. DEFINITIONS

1.1 **"Affiliate"** means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

1.2 **"Agreement**" means the written or electronic agreement between Customer and Duo Security for the provision of the Services to Customer.

1.3 "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The terms "**Controlled**" and "**Controlling**" will be construed accordingly.

1.4 "**Controller Affiliate**" means any of Customer's Affiliate(s) (a) (i) that are subject to applicable Data Protection Laws and (ii) permitted to use the Service pursuant to the Agreement between the Customer and Duo Security, but have not signed their own Order Form and are not a "Customer" as defined under the Agreement, and (b) if and to the extent Duo Security processes Personal Data for which such Affiliate(s) qualify as the Controller. Except where otherwise indicated, the term "Customer" shall include Customer and Controller Affiliate(s), if any.

1.5 "**Customer Data**" means any Personal Data that Duo Security processes on behalf of Customer pursuant to the Agreement and this DPA in the course of providing Services. Customer Data shall exclude Performance Data.

1.6 **"Data Breach"** means any unauthorized or unlawful breach of security that actually leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

1.7 **"Data Protection Laws"** means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

1.8 **"Data Controller"** means an entity that determines the purposes and means of the processing of Personal Data.

1.9 **"Data Processor"** means an entity that processes Personal Data on behalf of a Data Controller.

1.10 **"EU Data Protection Law"** means on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council 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) ("**GDPR**").

1.11 "**Group**" means any and all Affiliates that are part of entities corporate group.

1.12 "**Model Clauses**" means the Standard Contractual Clauses for Processors as approved by the European Commission and in the form set out in Annex B**.**

1.13 **"Personal Data"** has the meaning given to it in the GDPR.

1.14 **"Processing"** has the meaning given to it in the GDPR and "process," "processes," and "processed" will be interpreted accordingly.

1.15 **"Services"** means any product or service provided by Duo Security to Customer pursuant to the Agreement.

1.16 **"Subprocessor"** means any Data Processor engaged by Duo Security or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Subprocessors may include third parties or members of the Duo Security Group.

2. SCOPE OF THIS DPA

2.1 **Scope of DPA:** This DPA applies where and only to the extent that: (i) Duo Security processes Customer Data on behalf of Customer in the course of providing Services to the Customer pursuant to the Agreement; and (ii) the Agreement between Duo Security and the Customer expressly incorporates this DPA by reference.

3. ROLES AND SCOPE OF PROCESSING

3.1 **Role of the Parties**: As between Duo Security and Customer, Customer is the Data Controller of Customer Data and Duo Security shall process Customer Data only as a Data Processor acting on behalf of Customer.

3.2 **Customer Processing of Customer Data**: Customer agrees that (i) it will comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to Duo Security; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary for Duo Security to process Customer Data pursuant to the Agreement and this DPA.

3.3 **Duo Security Processing of Customer Data**: As a Data Processor, Duo Security will process Customer Data only for the purpose of providing the Services and in accordance with Customer's documented lawful instructions as set forth in the Agreement and this DPA. The parties agree that the Customer's complete and final instructions with regard to the nature and purposes of the processing are set out in this DPA. Processing outside the scope of these instructions (if any) will require prior written agreement between Customer and Duo Security on additional instructions for processing.

3.4 **Details of Data Processing**:

Subject matter: The subject matter of the data processing under this Addendum is the Customer

Data.

Duration: As between Duo Security and Customer, the duration of the data processing under this DPA is the term of the Agreement.

Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Customer.

Nature of the processing: Cloud based access security solutions, two-factor authentication technology and such other Services, as described in the Agreement.

Types of Customer Data: The types of Customer Data are determined by Customer in its sole discretion and may include but are not limited to: identification and contact data (name, address, title, job title, contact details, username); device data; financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility); and IT information (IP addresses, usage data, cookies data, device specific information, connection data, location data).

Categories of data subjects: The categories of data subjects whose personal data may be transferred in connection with the Services are determined and controlled by Customer in its sole discretion and may include but are not limited to: prospects, customers, business partners and vendors of Customer (who are natural persons); employees or contact persons of Customer's prospects, customers, business partners and vendors; employees, agents, advisors, freelancers of Customer (who are natural persons); Customer's end-users authorized by data exporter to use the Services.

3.5 **Analytics**: Notwithstanding anything to the contrary in the Agreement (including this DPA), the Customer acknowledges and agrees that, in the course of providing its Services, Duo Security may from time to time use and process data (including Personal Data) for the purposes of creating statistics and analytics data (including, but not limited to, Performance Data). Duo Security will use such data for the purposes described in Duo Security's Privacy Policy (available at https://duo.com/legal/privacy), which purposes include maintaining and improving the Services and monitoring and analyzing its activities in connection with the performance of the Services. Duo Security shall ensure that: (i) any such data is effectively anonymized, pseudonymized and/or aggregated data so that it does not reveal the specific identity of any individual; and (ii) its use of such data will comply with applicable laws. Subject to complying with this Section 3.5, nothing in the Agreement (including this DPA) shall prevent or restrict Duo Security from using or sharing any such data.

4. SUBPROCESSING

4.1 **Authorized Subprocessors**: Customer agrees that in order to provide the Services set forth in the Agreement, Duo Security may engage Subprocessors to process Customer Data. Duo Security maintains an up-to-date list of its authorized Subprocessors, which it updates on a regular basis. Duo Security's list of authorized Subprocessors can be found at https://duo.com/legal/subprocessors.

4.2 **Subprocessor Obligations**: Where Duo Security authorizes any Subprocessor as described in Section 4.1:

(a) Duo Security will restrict the Subprocessors access to Customer Data only to what is necessary to assist Duo Security in providing or maintaining the Services, and will prohibit the Subprocessor from accessing Customer Data for any other purpose;

(b) Duo Security will enter into a written agreement with the Subprocessor imposing data protection terms that requires the Subprocessor to protect the Customer Data to the standard required by Data Protection Laws; and

(c) Duo Security will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause Duo Security to breach any of its obligations under this DPA.

4.3 Duo Security will provide Customer with reasonable prior notice if it intends to replace any Subprocessors. Customer may object in writing to Duo Security's appointment of a new or replacement of an old Subprocessor, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution and if this is not possible, Customer may suspend or terminate the Agreement (without refund of any fees paid, prepaid or invoiced prior to suspension or termination).

5. SECURITY MEASURES AND DATA BREACH RESPONSE

5.1 **Security Measures**: Duo Security has implemented and will maintain appropriate technical and organizational security measures to protect Customer Data from Data Breaches and to preserve the security and confidentiality of the Customer Data ("**Security Measures**"). The Security Measures applicable to the Services are set forth in Annex A, as updated or replaced from time to time in accordance with Section 5.2.

5.2 **Updates to Security Measures**: Customer acknowledges that the Security Measures are subject to technical progress and development and that Duo Security may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

5.3 **Personnel:** Duo Security restricts its personnel from processing Customer Data without authorization by Duo Security as set forth in Annex A, and shall ensure that any person who is authorized by Duo Security to process Customer Data is under an appropriate contractual obligation of confidentiality.

5.4 **Customer Responsibilities**: Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

5.5 **Data Breach Response:** Upon becoming aware of a Data Breach, Duo Security will notify Customer without undue delay and will provide information relating to the Data Breach as it becomes known or as is reasonably requested by Customer. Duo Security will also take reasonable steps to mitigate and, where possible, to remedy the effects of, any Data Breach.

6. AUDIT REPORTS

6.1 **Audit Reports:** Duo Security audits its compliance against data protection and information security standards (currently, a SOC 2 Type II audit) on a regular basis. Such audits are conducted by independent, experienced personnel, and may include Duo Security's internal audit team and/or third party auditors engaged by Duo Security. Upon Customer's request, Duo Security will provide Customer with details of the audits it conducts relevant to the Services it is providing to Customer and, if required, supply customer with an accurate summary of its most recent relevant audit report ("**Report**") so that Customer can verify Duo Security's compliance with this DPA. Duo Security will further answer all reasonable questions related to data protection that Customer may have in connection with the Report in a prompt and timely manner. Customer is responsible for reviewing the information made available by Duo Security relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under applicable laws.

6.2 **Confidentiality of Audit Reports**: The Customer acknowledges that the Report will constitute Duo Security's Confidential Information and will protect the Report in accordance with the confidentiality provisions of the Agreement.

6.3 **Customer Audits:** Customer agrees to the provision of the Report by Duo Security in fulfilment of any audit cooperation responsibilities that may apply to Duo Security under Data Protection Laws. Notwithstanding the foregoing, if Customer reasonably believes that an audit is necessary to meet its obligations under any applicable Data Protection Laws, Customer may request that a third-party (at Customer's expense) conduct an audit and Duo Security will work with Customer to the extent feasible to accommodate Customer's request. If Duo Security is unable to accommodate Customer's request, Customer is entitled to terminate this DPA and the Agreement. Where the Model Clauses apply, nothing in this Section 6.3 varies or modifies the Model Clauses nor affects any supervisory authority's or data subject's rights under the Model Clauses.

7. TRANSFERS OF PERSONAL DATA

7.1 **Data center locations:** Duo Security may transfer and process Customer Data anywhere in the world where Duo Security its Affiliates or its Subprocessors maintain data processing operations. Duo Security shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

7.2 **Application of Model Clauses**: To the extent that Duo Security processes any Customer Data protected by EU Data Protection Law under the Agreement and/or that originates from the European Economic Area (including the United Kingdom) ("EEA") or Switzerland, in a country

that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that Duo Security shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by complying with the Model Clauses. Duo Security agrees that it is a "data importer" and Customer is the "data exporter" under the Model Clauses (notwithstanding that Customer may be an entity located outside of the EEA).

7.3 **Alternative Data Export Solutions:** Notwithstanding the foregoing Section 7.2, the parties agree that in the event Duo Security adopts Binding Corporate Rules or another alternative data export solution (as recognized under EU Data Protection Laws), then the Model Clauses will cease to apply with effect from the date that Duo Security implements such new data export solution.

8. RETURN OR DELETION OF DATA

8.1 Following expiration of the Agreement, Duo Security shall delete or return to Customer all Customer Data in its possession in accordance with the terms of the Agreement and save to the extent Duo Security is required by applicable law to retain some or all of the Customer Data (in which case, Duo Security shall implement reasonable measures to isolate the Customer Data from any further processing).

9. COOPERATION

9.1 The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Duo Security shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to Duo Security, Duo Security shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Duo Security is required to respond to such a request, Duo Security will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

9.2 If a law enforcement agency sends Duo Security a demand for Customer Data (for example, through a subpoena or court order), Duo Security will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Duo Security may provide Customer’s basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Duo Security will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Duo Security is legally prohibited from doing so.

9.3 To the extent Duo Security is required under EU Data Protection Laws, Duo Security will (at Customer's expense) provide reasonably requested information regarding the Services to enable

the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

10. GENERAL

10.1 For the avoidance of doubt, any claim or remedies the Customer may have against Duo Security, any of its Affiliates and their respective employees, agents and subprocessors arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; (iii) under EU Data Protection Laws, including any claims relating to damages paid to a data subject; and (iv) breach of its obligations under the Model Clauses, will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Customer further agrees that any regulatory penalties incurred by Duo Security in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Duo Security's liability under the Agreement as if it were liability to the Customer under the Agreement. Nothing in this DPA is intended to limit the Parties' direct liability towards data subjects or applicable supervisory data protection authorities.

10.2 Any claims against Duo Security or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

10.3 No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms**.**

10.4 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

10.5 In the event of any conflict between this DPA and any privacy-related provisions set out in the Agreement or any other existing data protection terms agreed to between the parties, the terms of this DPA shall prevail.

10.6 This DPA is provided in a pre-printed, pre-signed and read-only electronic form published by Duo Security. Any modification of the provisions or terms of this DPA will be considered to make the pre-signatures below null and void. In the event that this DPA contains modifications, even if signed by the representatives of Duo Security other than an authorised signatory, such modifications shall be null and void and this DPA shall be construed as if such modifications had not been made.

IN WITNESS WHEREOF, the **parties have caused** this DPA to be executed by their authorized representative:

Duo Security, Inc.

By: Jim Cyb (Nov 19, 2018)

Name: Jim Cyb

Title: VP Sales - Global Secure Access

Date: Nov 19, 2018

Customer

By: _____

Name: _____

Title: _____

Date: _____

ANNEX A

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES TO BE IMPLEMENTED BY DUO SECURITY

Duo provides Annex A to customers under a valid Agreement, and to prospective customers under a confidentiality agreement. Please email GDPR@duo.com for a copy.

ANNEX B
MODEL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the **data exporting** organisation:

The identity identified as the "data exporter" in Appendix 1 of these Contractual Clauses

(**the data exporter**)

And

Name of the **data importing** organisation:

Duo Security, Inc.,

Address: 123 N Ashley St #200, Ann Arbor, MI 48104

Tel: (866) 760-4247

Email: counsel@duosecurity.com

(**the data importer**)

each a "**party**"; together "**the parties**".

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

'personal data', '**special categories of data'**, '**process/processing'**, '**controller'**, '**processor'**, '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

'the data exporter' means the controller who transfers the personal data;

'the data importer' means the processor who agrees to receive from the data exporter personal

data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which

case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(i) any accidental or unauthorised access, and

(ii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same

conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Subprocessing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

11.2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter / Description of Customer

The data exporter is (please specify briefly activities relevant to the transfer):

*The data exporter is: (i) the legal entity that is identified as "Customer" and who has executed these Standard Contractual Clauses, and, (ii) all members of the Customers Group (as defined in the data processing agreement between the data exporter and data importer) established within the European Economic Area (including United Kingdom) (EEA) and Switzerland that have purchased a subscription for the data importers services as set forth in the underlying agreement for services between the data exporter and the data importer (the "**Agreement**')*

Data importer / Nature of Services provided by Duo Security

The data importer is (please specify briefly your activities relevant to the transfer):

*Duo Security, Inc. provides cloud based access security solutions and two-factor authentication technology which involves processing Personal Data provided by, and pursuant to the instructions and directions of Customer, in accordance with the terms of the Agreement ("**Services**").*

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

- *Prospects, customers, business partners and vendors of data exporter (who are natural persons)*
- *Employees or contact persons of data exporter's prospects, customers, business partners and vendors.*
- *Employees, agents, advisors, freelancers of data exporter (who are natural persons)*
- *Customer's end-users authorized by data exporter to use the Services*

Categories of data

The personal data transferred concern the following categories of data (please specify):
Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by Data Exporter in its sole discretion, and which may include, but is not limited to, the following types of Personal Data:

- *Identification and contact data (name, address, title, contact details),*
- *Financial information (credit card details, account details, payment information)*
- *Employment details (employer, job title, geographic location, area of responsibility)*
- *IT information (IP addresses, usage data, cookies data, device specific information, connection data, location data)*

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

The Services are not designed to require the submission of special categories of Personal Data. Therefore, it is not anticipated that data exporter will submit special categories of Personal Data to the Services, and to the extent such data is submitted to the Services, it is determined and controlled by data exporter in its sole discretion.

Nature of Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by Duo Security is the performance of the Services pursuant to the Agreement.

Duration of Processing Operations:

The term of the Agreement.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The security measures are described in Annex A of the Data Protection Addendum.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's confidential information as such term is defined in the Agreement (defined in Appendix 1) and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions in accordance with and as described in Section 3.3 of the Data Protection Addendum incorporating these Clauses (the "**DPA**")

2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").

4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described Section 6 (Audit Reports) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.

2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with Section 4 (Subprocessing) of the DPA.

DATA EXPORTER

Name:……..

Authorised Signature ……

DATA IMPORTER

Name: Jim Cyb ……..

Authorised Signature Jim Cyb (Nov 19, 2018) ……