INTRODUCTION

At Zype, our mission is to help our customers build awesome video products and services. Because optimizing our customers' data is such an integral part of our service offerings, we understand the importance of protecting data and ensuring that our agreements meet your needs, including the need to demonstrate compliance with regulatory requirements. For this reason, we created our Data Processing Agreement to help you demonstrate compliance with data privacy and security requirements, as well as to streamline the onboarding process. In particular, this agreement provides our customers with a number of important assurances, such as:

- We put you in control of your data, because we will collect, use, and share your data only in accordance with your instructions as outlined in our agreement;
- We maintain physical, technical, and administrative security measures to protect and safeguard customer data;
- We respect your need to demonstrate compliance with privacy and security laws, and we will work together with you to protect your data; and
- We will not, under any circumstances, sell any data you have provided to us.

Through the obligations we undertake in this Data Processing Agreement, we provide our customers with peace of mind that we will always handle the data entrusted to us with care and respect.

Please do not provide us with the personal data of European Union residents until after you have provided us with written notice and we have signed the Standard Contractual Clauses required by data privacy regulations in the European Union.

DATA PROCESSING AGREEMENT

This Data Processing Agreement (this "**DPA**") forms part of the Zype Master Terms and Conditions ("**Agreement**") between Zype Inc. ("**Company**") and [INSERT CONTROLLER PARTY] ("**Customer**") (Company and Customer are referred to herein individually as "Party" and collectively as the "Parties") entered into XX day of [Month], [Year] ("**Effective Date**").

All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In providing services to Customer pursuant to the Agreement (the "**Services**"), Company may Process Customer Data on behalf of Customer, and the parties agree to comply with the following provisions with respect to any Customer Data. The Parties acknowledge that this DPA reflects the Parties' agreement with regard to the Processing of Customer Data.

1.   **Definitions**

1.1   "**Customer Data**" means all Personal Information that is, in relation to the Services: (i) provided by or on behalf of Customer to Company; or (ii) obtained or Processed by Customer (including its agents and subcontractors) by or for the benefit of Company.

1.2   "**Data Subject**" means an identified, or identifiable, natural person to whom Personal Information relates.

1.3   "**Personal Information**" means any information that identifies, relates to, describes, or is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household, or is otherwise "personal data," "personal information," "personally identifiable information," "nonpublic personal information," "protected health information," or similar designation under and regulated by Privacy Law.

1.4 "**Privacy Law**" means all applicable federal, state, territorial, and local laws, rules, directives, regulations, and governmental requirements currently in effect, or as they become effective, relating in any way to the privacy, confidentiality, or security of Personal Information, including, to the extent relevant, the California Consumer Privacy Act of 2018, Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code ("**CCPA**"), the General Data Protection Regulation 2016/679 ("**GDPR**"), and any equivalent or similar laws, rules, regulations, and governmental requirements in applicable jurisdictions, and any laws implementing, replacing or supplementing any of them, as amended, consolidated, re-enacted, or replaced from time to time.

1.5 "**Process(ing)**" means the collection, use, modification, storage, disclosure and any other activity with respect to Personal Information that is governed by Privacy Law.

1.6 "**Sell(ing)**" has the meaning ascribed to it in the CCPA.

1.7 "**Service Provider**" has the meaning ascribed to it in the CCPA.

2. **Processing Location and Standard Contractual Clauses**

2.1 Company will Process Customer Data in [insert country/countries]. In the event that the Company intends to change the country/countries it processes Customer Data, the Parties shall amend this DPA in writing to reflect such change. Where required by Privacy Law, the Parties will enter into standard contractual clauses in Exhibit A herein, or other similar documentation required for the international transfer of Personal Information, to ensure an adequate level of data protection ("**Standard Contractual Clauses**").

2.2 In the event of a change in any Privacy Laws relating to the country/countries where an adequate level of data protection exists, the Parties will discuss, and agree on, an alternative solution permitting the Company to continue to Process the Personal Information in said country/countries.

2.3 In the case of any inconsistency between any of the provisions of the Agreement, this DPA, and the Standard Contractual Clauses respectively, the provisions of the Standard Contractual Clauses shall prevail in preference to the Agreement and this DPA, and the provisions of this DPA shall prevail over the provisions of the Agreement.

3. **Customer's Instructions**

3.1 Customer has the sole right to give Company instructions regarding the Processing of Customer Data. Customer hereby instructs Company to process Customer Data to the extent required to provide the Services. Customer's instructions will regularly be given in writing. Oral instructions will be confirmed in writing as soon as possible.

3.2 If in Company's opinion, the execution of an instruction of Customer would breach this DPA, the Standard Contractual Clauses (if any), or Privacy Laws, Company will notify Customer in writing. In such a case, Company will suspend the execution of the instruction until the instruction is confirmed by Customer in writing.

4. **General Obligations of Customer**

4.1 Customer is the controller of Customer Data (as the term controller is defined within applicable Privacy Law).

4.2 Customer represents and warrants that it has obtained Customer Data in compliance with applicable Privacy Law and that providing Customer Data to Company pursuant to the Agreement shall not cause Company to be in violation of applicable Privacy Law.

4.3 Customer will notify Company as soon as possible of any errors or irregularities (if any) it discovers in connection with the Processing of Customer Data by Company.

5. **General Obligations of Company**

5.1 Company is the processor of Customer Data (as the term processor is defined within applicable Privacy Law).

5.2 Where applicable under Privacy Law, Company is a Service Provider to Customer and Company certifies that it understands the restrictions set forth in the CCPA and agrees that:

5.2.1 Company shall Process all Customer Data on behalf of Customer only;

5.2.2 Company is prohibited from retaining, using, or disclosing Customer Data for any purpose other than for the specific purpose of performing the Services, including, without limitation, from retaining, using, or disclosing such Customer Data (a) for a purpose other than providing the Services (b) outside of the direct business relationship between the relevant Data Subject and Customer (and Company on behalf of Customer);

5.2.3 Company shall not further collect, use, or disclose Customer Data except as necessary to perform the Services; and

5.2.4 Company is prohibited from Selling Customer Data for any reason.

5.3 Company will only process Customer Data in accordance with the instructions provided by Customer, this DPA, the Standard Contractual Clauses (if any), and Privacy Law.

5.4 Company shall, however, have the right to Process the Customer Data outside the scope set out in Section 5.3: (i) in the case of the Personal Information of Data Subjects resident in the European Union, as may be required by the laws of the European Union or its members states; (ii) in the case of the Personal Information of Data Subjects not resident in the European Union, as may be required by any country's laws to which Company is subject to; and (iii) for the permitted service provider uses listed in the California Attorney General's California Consumer Privacy Act Regulations (as may be amended from time to time).

5.5 Company will provide Customer with assistance, as Customer may reasonably request and at Customer's sole cost, to enable Company to comply with obligations imposed on Customer in relation to Customer Data, including, but not limited to, providing any assistance with Data Subject rights requests, data protection impact assessments, and prior consultations of Company required under Privacy Law, or other binding legal obligations, which may include, litigation holds and responding to binding orders of a court or regulatory authority with jurisdiction.

5.6 Company shall inform Customer as soon as possible, in writing, of any inquiry, complaint, notice, or other communication it receives from any supervisory authority or other governmental body or any individual, relating to Customer's compliance with Privacy Law. Company shall present to Customer, upon request, such complaints, notice, or other communication and shall provide reasonable assistance to Customer, at Customer's sole cost, to enable Customer to respond to such inquiries, complaints, notices, or other communications. For the avoidance of doubt, Company shall not respond to any such inquiry, complaint, notice, or other communication without the prior written consent of Customer (unless otherwise required by applicable law).

5.7 Company will notify Customer as soon as possible, and as far as it is legally permitted to do so, of any access request for disclosure of data which concerns Customer Data (or any part thereof) by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction. For the avoidance of doubt, and as far as it is legally permitted to do so, Company shall not disclose or release any Customer Data in response to such request served on Company without first consulting with, and obtaining the written consent of, Customer.

6. **Data Protection and Security**

6.1 Company has designated or will designate a data protection officer and/or a representative in the EU and/or any other jurisdiction to the extent required under Privacy Law. Company will notify Customer, in writing, of

(and of any changes to) the identity and contact details of any data protection officer and/or representative (if any) as soon as possible.

6.2   Company will maintain a record of all categories of Processing activities carried out on behalf of Customer to the extent required to enable Customer to comply with its obligations under Privacy Law. Company will cause each sub-processor it retains to maintain a record of all categories of Processing activities carried out on behalf of the Company by the sub-processor to the extent required to enable Customer or Company to comply with its obligations under Privacy Law. The records in this Section 6.2 include, without limitation:

6.2.1   a description of the categories of the Customer Data being processed and the categories of the Processing activities undertaken;

6.2.2   details of any transfer of Customer Data, including details of: (i) the country in which the recipient is located and, if applicable, the recipient international organization; and (ii) the safeguards implemented for the protection of Customer Data; and

6.2.3   a general description of the technical and organizational security measures implemented pursuant to Section 6.6.

6.3   Company shall make available (and shall cause any sub-processor to make available) to Customer copies of such records in electronic form upon reasonable request from the Customer.

6.4   Company will ensure the reliability of any person authorized to process Customer Data and ensure that such persons have committed themselves in writing to confidentiality or are under an appropriate obligation of confidentiality and an obligation to act in compliance with Privacy Law.

6.5   Company shall keep Customer Data confidential and implement and maintain (and required any sub-processors that have access to Customer Data to maintain) a documented information security program appropriate to the nature of the Customer Data that: (a) contains administrative, technical, and physical safeguards to identify, assess and protect against any reasonably foreseeable anticipated or actual threats or hazards (whether internal or external) to the security or integrity of Customer Data (including threats of loss, theft, unauthorized access, use, disclosure or other unauthorized processing of Customer Data or any failure of security controls protecting Customer Data), whether contained in tangible or intangible records ("**Safeguards**"); (b) meets commercially reasonable standards for such Safeguards; and (c) complies with Privacy Law.

6.6   Company shall (a) proactively monitor and assess risks and the sufficiency of any Safeguards in place to control such risks; (b) review the scope of security measures at least annually and when a material change in Company's business practices occurs that may reasonably implicate the security or integrity of records containing Customer Data; and (c) implement and maintain Safeguards to control the risks Company identifies through risk assessment, regular testing, and otherwise monitoring the effectiveness of the Safeguards' key controls, systems and procedures to confirm the information security program is operating in a manner that is reasonably calculated to prevent and detect unauthorized access to or use or disclosure of Customer Data. Company will periodically improve such Safeguards in line with the new development of best practices and technical standards.

7.   **Data Breach Notification**

7.1   Company shall notify Customer as soon as possible, and in any event no later than 24 hours, after the discovery of any breach of security that resulted in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Customer Data transmitted, stored, or otherwise Processed by Company or any of its sub-processors. The notification shall at least:

7.1.1   describe the nature of the data breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Customer Data records concerned; and

7.1.2 describe the measures taken or proposed to be taken to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where it is not possible to provide all of the information at the same time, the information may be provided in phases.

7.2 Company shall provide reasonable assistance, upon Customer's request, with any obligation of Customer under Privacy Law to document any such data breach. If the data breach is directly attributable to the actions of Customer, any reasonable assistance provided by Company shall be at Customer's sole cost and expense.

8. Rights of the Data Subjects

8.1 Customer shall have sole discretion in responding to the rights asserted by the Data Subjects. Company will forward to Customer any requests of Data Subjects in connection with Customer Data.

8.2 Company will reasonably assist Customer, upon request and at Customer's sole cost, in fulfilling any rights of the Data Subjects to the extent these rights relate to the Processing of Customer Data by Company.

9. Data Upon Termination

9.1 Upon Customer's request, at the latest, however, upon termination or expiration of the Agreement, Company will, at the choice of Customer, while respecting data protection and security measures, delete or return to the Customer all Customer Data and delete all existing copies unless: (a) in the case of the Personal Information of Data Subjects resident in the European Union, the laws of the European Union or its members states require a longer retention period; and (b) in the case of the Personal Information of Data Subjects not resident in the European Union, the country's laws to which Company is subject to require a longer retention period.

10. Right to Engage Sub-processors

10.1 Customer has instructed and authorized the use of sub-processors to assist Company with respect to the performance of Company's obligations under the Agreement and Company agrees to be responsible for the acts or omissions of such sub-processors to the same extent as Company would be liable if performing the services of the sub-processors under the terms of this DPA. Upon written request of Customer, Company will provide to Customer a list of its then-current sub-processors.

10.2 Where Company engages another party in accordance with this DPA, obligations providing for at least for an equal level of data protection, as established by this DPA, shall be imposed on that other party by way of a written contract, such as a data processing agreement.

11. Liability

11.1 Each Party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the section of the Agreement that describes each Party's liability.

12. Audits and Inspections

12.1 Customer (itself or through a third party) has the right to inspect or audit, at Customer's sole cost, Company's compliance with this DPA. Company will grant Customer, or a designated third party, access to its business premises during the Company's regular business hours and make available all information necessary to demonstrate compliance with this DPA; *provided*, *however*, that such audit or inspection shall be conducted in a manner designed to cause minimal interruption to Company's business operations.

12.2   Customer will notify Company, in writing, of any such audit or inspection at least eight (8) weeks in advance. Customer may not conduct more than one audit or inspection per calendar year unless otherwise required by applicable Privacy Law.

12.3   Company will provide reasonable assistance, at Customer's sole cost and as reasonably requested by Customer, in connection with any audits of any competent supervisory or regulatory authority to the extent such audit relates to the Processing of Customer Data by Company under this DPA.

12.4   Company shall ensure that similar provisions are included in its agreements with sub-processors.

13.   **Final Provisions**

13.1   This DPA is subject to the laws of the jurisdiction as stated in the Agreement. The Parties exclusively submit to the courts of the chosen jurisdiction as set out in the Agreement.

13.2   Any amendments or supplements to, or termination of, this DPA must be in writing in order to be legally effective, this requirement applies accordingly to any waiver of this written form requirement. For the avoidance of doubt, any references to any written form requirement in this DPA (e.g. "written" or "in writing") include declarations and documents in electronic and text form whether bearing a signature or not (e.g. emails, fax copies or scans).

13.3   If a provision of this DPA is or becomes ineffective, in whole or in part, or if there is an omission, the remaining provisions of this DPA shall remain unaffected. In place of the ineffective provision, and to fill the omission, the Parties will, in good faith, agree on a reasonable provision which comes - to the extent legally possible - closest to what the Parties agreed or would have agreed if they had considered this point.

IN WITNESS WHEREOF, the parties hereto have signed this DPA as of the day and year first above written intending to be legally bound hereby.

ZYPE INC.   **[INSERT CUSTOMER]**

_____   _____

Name: Name:

Title: Title:

Date: Date:

EXHIBIT A

STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC and Article 46(1) of Regulation (EU) 2016/679 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 organization: [insert customer]

Address: [insert customer]

Attn: [insert contact]

[Insert address]

[Insert address]

Tel.: _____ fax: _____ e-mail: _____

Other information needed to identify the organization: _____

(each and all the data **exporter**)

and

Name of the data importing organization: Zype Inc.

Address: Zype Inc.

Attn: [insert contact]

[insert address]

[insert address]

Tel.: _____ fax: _____ e-mail: _____

Other information needed to identify the organization: _____

(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. From and after 25 May, 2018, any reference to Directive 95/46/EC shall be a reference to the applicable provision of Regulation (EU) 2016/679.

Clause 1

Definitions

For the purposes of the Clauses:

(a)   *'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;

(b)   '*data exporter*' means the controller who transfers the personal data;

(c)   *'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;

(d)   *'sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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;

(e)   *'applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of natural persons 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;

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

Clause 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.

Clause 3

Third-party beneficiary clause

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.

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.   The data subject can enforce against the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

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.

Clause 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 organizational 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, unauthorized 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 sub-processor 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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).

Clause 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 organizational 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,

(ii)   any accidental or unauthorized access, and

(iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

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

Clause 6

Liability

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 sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

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 sub-processor 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.

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

3.	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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

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.

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.

Clause 8

Cooperation with supervisory authorities

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.

2.	The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, 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.

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

Clause 9

Governing Law

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

Clause 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.

Clause 11

Sub-processing

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.

2.   The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for sub-processing 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.

4.   The data exporter shall keep a list of sub-processing 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.

Clause 12

Obligation after the termination of personal data processing services

1.   The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor 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.

2.   The data importer and the sub-processor 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.

On behalf of the data exporter:

Name (written out in full): _____

Other information necessary in order for the contract to be binding (if any):

Signature: _____

<div style="text-align: right;">(stamp of organization)</div>

On behalf of the data importer:

Name (written out in full): _____

Other information necessary in order for the contract to be binding (if any):

Signature: _____

<div style="text-align: right;">(stamp of organization)</div>

Appendix 1 to the Standard Contractual Clauses

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

Data exporter

(please briefly explain the activities relevant to the transfer):

The data exporter is providing Personal Information (as defined in the DPA) from the Data Subjects to the data importer for the purpose of obtaining the Services (as defined in the DPA). This may include data transfers from the data exporter to the data importer using media or electronic transmission, on public or private networks, across national borders, and both within and without the European Union member states.

Data importer

(please briefly explain the activities relevant to the transfer):

The data importer is receiving Personal Information (as defined in the DPA) from the data exporter for the purpose of providing the Services (as defined in the DPA) to the data exporter. This may include data transfers from the data exporter to the data importer using media or electronic transmission, on public or private networks, across national borders, and both within and without the European Union member states.

Data Subjects

The Personal Information transferred include the following categories of Data Subjects (please specify):

- *Employees, contractors, temporary/agency workers, and consultants;*

- *Customers; and*

- *Other third parties including representatives of and contacts at vendors, licensees, franchisees, and other business partners.*

All of the above categories include current, past, and prospective Data Subjects.

Categories of data

The Personal Information transferred include the following categories of data (please list):

Special categories of data (if appropriate)

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

- *Data concerning health;*

- *Criminal convictions;*

- *Religious beliefs; and*

- *Trade union membership.*

Processing operations

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

The basic processing activities are as described in the Agreement and the DPA and include the following:

The objective of Processing of Personal Information by the data importer is the performance of the Service pursuant to the Agreement.

Processing locations

The Personal Information transferred will be processed in the following countries/locations (please specify):

United States of America

On behalf of the data exporter:

Name (written out in full): _____

Other information necessary in order for the contract to be binding (if any):

Signature: _____

(stamp of organization)

On behalf of the data importer:

Name (written out in full): _____

Other information necessary in order for the contract to be binding (if any):

Signature: _____

(stamp of organization)

Appendix 2 to the Standard Contractual Clauses

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

The following is a description of the technical and organizational security measures implemented by the data importer in accordance with the DPA and Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer shall maintain administrative, physical and technical safeguards for protecting the security, confidentiality and integrity of Customer Data, as described in the DPA.

On behalf of the data exporter:

Name (written out in full): _____

Other information necessary in order for the contract to be binding (if any):

Signature: _____

(stamp of organization)

On behalf of the data importer:

Name (written out in full): _____

Other information necessary in order for the contract to be binding (if any):

Signature: _____

(stamp of organization)