## Data Processing Addendum

This Data Processing Addendum ("**Addendum**") forms part of the Services Agreement or other agreement between the Customer and Bold Innovation Group Ltd. ("**Bold Commerce**"), for the provision of IT or data processing services by Bold Commerce to the Customer (the "**Services Agreement**"). Each of the Customer and Bold Commerce shall be a "**Party**", and shall be collectively referred to as the "**Parties**".

By executing this Addendum, the Customer enters into this Addendum on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates, if and to the extent Bold Commerce processes Personal Data for which such Affiliates qualify as the Controller. For the purposes of this Addendum only, and except where indicated otherwise, the term "**Customer**" shall include Customer and Affiliates.

**Whereas:**

A. The performance of services pursuant to the Services Agreement may require Bold Commerce to process Personal Data of end customers located in the European Economic Area (**EEA**) or the UK on behalf of the Customer;

B. The Customer and Bold Commerce each have obligations to observe and comply with data protection laws and regulations including, but not limited to the, the EU General Data Protection Regulation (**GDPR**) the UK GDPR and applicable Swiss Law.

C. In its performance of services pursuant to the Service Agreement, Bold Commerce will act as a Processor for the purposes of processing Personal Data on behalf of the Customer (the Controller), and the processing of such data will be governed by this Addendum;

D. This Addendum shall apply as follows:
   (i) If the Customer entity signing this Addendum is a party to the Services Agreement, this Addendum is an addendum to and forms part of the Services Agreement;
   (ii) If the Customer entity signing this Addendum has executed an Order Form with Bold Commerce pursuant to the Services Agreement, but is not itself a party to the Services Agreement, this Addendum is an addendum to that Order Form and applicable renewal Order Forms;
   (iii) If the Customer entity signing this Addendum is neither a party to an Order Form nor the Services Agreement, this Addendum is not valid and is not legally binding. That entity should therefore request that the Customer entity who is a party to the Services Agreement executes this Addendum; and

E. This Addendum will be executed as follows:
   (i) This Addendum consists of two parts: the main body of the Addendum, and the attached Appendixes and Exhibits;
   (ii) This Addendum has been pre-signed on behalf of Bold Commerce, and the Standard Contractual Clauses attached hereto have been (to the extent that is practicable) pre-populated and pre-signed by Bold Commerce on behalf of its affiliate in the United States, Bold Commerce, Inc., as the data importer;
   (iii) To complete and execute this Addendum, the Customer must complete the information in the signature box and sign on Pages 8, 21, 49, 60, 61 and 62 complete the information as the data exporter on Page 20, complete the information required in Pages 24, 27, 28, 43, 49, and 50 and

send the completed and signed Addendum to Bold Commerce by email to **privacy@boldcommerce.com**; and

(iv) Upon receipt of the validly completed Addendum by Bold Commerce at this email address, this Addendum will become legally binding.

**In furtherance of the above, the Parties hereby agree as follows:**

**1.0 Interpretation**

1.1 The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Services Agreement. Except as modified below, the terms of the Services Agreement shall remain in full force and effect.

1.2 "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer, and which is subject to the data protection laws of the European Union and/or the UK and is permitted to use the services provided by Bold Commerce to the Customer pursuant to the Services Agreement. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.3 "**Claim**" means any third party action, claim, assertion, demand or proceeding.

1.4 "**Consent**" means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

1.5 "**Controller**" means the entity which determines the purposes and means of the processing of Personal Data. For the purposes of this Addendum, the Customer is a Controller.

1.6 "**Data Protection Laws**" means the GDPR and, to the extent applicable, the data protection or privacy laws of any other country or territory.

1.7 "**Data Subject**" means an individual or natural person to whom Personal Data relates.

1.8 "**GDPR**" means the General Data Protection Regulation, EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

1.9 "**Personal Data**" means any information relating to an identified/identifiable Data Subject, an identifiable "**Data Subject**" being one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data may include, but is not limited to, name, address, phone number, email address, IP address and other identifying information.

1.10 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

1.11 "**Processing**" or "**Process**" means any operation, or set of operations, performed on Personal Data during the provision of a service, whether or not by automated means. Processing may include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12 "**Processor**" means an entity or person that processes data on the behalf of the Controller. For the purposes of this Addendum, Bold Commerce is a Processor.

1.13 "**Profiling**" means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

1.14 "**Pseudonymisation**" means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information.

1.15 "**Sub-Processor**" means an entity engaged by the Processor to process personal data on Processor's behalf.

1.16 "**Supervisory Authority**" means an independent public authority which is established in a relevant country or territory and is concerned by/with the Processing of Personal Data.

## 2.0    Personal Data Processing

2.1    Each Party acknowledges that it has obligations under the Data Protection Laws, and that it is solely responsible for compliance with same.

2.2    Bold Commerce shall comply with all applicable Data Protection Laws in the Processing of Personal Data, and not Process Personal Data other than pursuant to the Customer's instructions, unless Processing is required by applicable laws to which Bold Commerce is subject, in which case Bold Commerce shall to the extent permitted by applicable law inform the Customer of that legal requirement before the relevant Processing of that Personal Data.

2.3    The Customer hereby instructs Bold Commerce (and authorizes Bold Commerce) to Process Personal Data provided by the Customer, and in particular, to transfer such Personal Data to any country or territory, as may be reasonably necessary for the provision of the services described in the Services Agreement. The Customer shall not submit or provide any Personal Data of a Data Subject to Bold Commerce at any time nor for any purpose without ensuring that it has Consent of that Data Subject (or, if applicable, another legal basis under the Data Protection Laws) to collect and Process the Personal Data as contemplated.

2.4    Additional detail regarding Bold Commerce's Processing of Personal Data is set out in Appendix 1. The Customer may make reasonable amendments to Appendix 1 by written notice to Bold Commerce from time to time as the Customer reasonably considers necessary to meet the requirements of applicable Data Protection Laws.

2.5    Bold Commerce shall take reasonable steps to ensure that access to Personal Data is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of the Services Agreement, and to comply with applicable laws in the context of that individual's duties to Bold Commerce, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

## 3.0    Security

3.1    Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity relating the rights and freedoms of natural persons, Bold Commerce shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and the measures outlined in Section 3.3 below.

3.2    In assessing the appropriate level of security, Bold Commerce shall take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

3.3    Bold Commerce has developed and maintains data and organizational security measures that are designed to secure Personal Data in accordance with the state of the art, including:

(a)    System access controls, and prevention of unauthorized persons from gaining access to information systems;

(b)     User roles and need-to-know access, and prevention of authorized persons from accessing data, including Personal Data, that is not relevant to the performance of their job functions;

(c)     Establishment and maintenance of audit trails in Bold Commerce information systems that log who accesses data, what data is accessed, when it is accessed, how it is accessed, and where it is accessed from;

(d)     Prevention of accidental destruction of Personal Data;

(e)     Ensuring any physical copies of documents containing Personal Data are securely stored and destroyed pursuant to Bold Commerce's Document Retention Policy; and

(g)     Use of data encryption with respect to certain categories of data, including sensitive data such as payment data; and

(h)     Use of non-disclosure and confidentiality agreements with employees and contractors as a condition of employment or engagement.

## 4.0     Data Subjects

4.1     Bold Commerce has no direct relationship with Data Subjects that may provide Personal Data to the Customer and shall inform Data Subjects to contact the Customer first in the event of questions or complaints regarding the Processing of their Personal Data. Bold Commerce shall notify the Customer, unless specifically prohibited by applicable laws and regulations, if Bold Commerce receives:

(a)     any requests from an individual with respect to Personal Data Processed, including but not limited to opt-out requests, requests for access and/or rectification, blocking, data portability and all similar requests;

(b)     any complaint relating to the Processing of Personal Data, including allegations that the Processing infringes on a Data Subject's rights under Data Protection Laws; or

(c)     any order, demand, warrant, or any other document purporting to compel the production of Personal Data under applicable law.

Bold Commerce shall not respond to any of the above unless expressly authorized to do so by the Customer, or as obligated under applicable law or a valid court order.

4.2     Bold Commerce shall reasonably cooperate with the Customer and assist the Customer with respect to any action taken relating to such request, complaint, order or other document as described under Section 4.1 above. As far as reasonably possible, and taking into account the nature of the Processing, the information available to Bold Commerce, industry practices and costs, Bold Commerce will implement appropriate technical and organizational measures to provide the Customer with such cooperation and assistance.

4.3     Where the Customer is obliged under Data Protection Laws to provide information to an individual or a Supervisory Authority about the collection, Processing or use of Personal Data, Bold Commerce shall reasonably assist the Customer in making this information available. Where the required information can be retrieved by the Customer itself from the systems of Bold Commerce through the access methods and reporting features made available by Bold Commerce to the Customer, the Customer shall retrieve such information itself from the systems of Bold Commerce.

4.4     Bold Commerce shall not be liable, and the Customer shall indemnify and hold harmless Bold Commerce, for any Claim or complaint from a Data Subject regarding any action by Bold Commerce taken as a result of instructions received from the Customer.

4.5     Data Subjects must provide Consent for the Processing of their Personal Data prior to completion of transactions using the Bold Commerce Services, and have the right to make certain requests or decisions regarding their Personal Data, which may include as applicable and appropriate:

(a)    Opting out of any automated Processing that may constitute Profiling;

(b)    Requesting that their Personal Data be erased; or

(c)    Opting out of further Processing of their Personal Data.

**5.0     Data Location**

5.1     Bold Commerce will store any Personal Data processed pursuant to the Services Agreement and this Addendum on servers located in the United States and Canada.  Bold Commerce will implement appropriate organizational and technical measures to ensure that Personal Data in transit receives adequate levels of protection as required by applicable law.

5.2     The Customer understands and agrees that Sub-Processors providing third party payment and other processing services involved in provision of services by Bold Commerce pursuant to the Services Agreement will store data within their relevant systems and servers located in the EU, United States, and/or Canada.

**6.0     Personal Data Breach**

6.1     In the case of a Personal Data Breach affecting any Personal Data provided by the Customer, Bold Commerce will notify the Customer without unreasonable delay, and in any event within 72 hours of discovering the Personal Data Breach, and provide sufficient information to allow the Customer to meet any obligations to report or notify Data Subjects or a Supervisory Authority of the Personal Data Breach under Data Protection Laws, including:

(a)    A description of the nature and scope of the Data Breach;

(b)    Name and contact details of Bold Commerce's breach response team;

(c)    Description of anticipated risks and results; and

(d)    Description of preventative and remedial steps taken by Bold Commerce to contain and address the breach.

6.2     The Customer will notify Bold Commerce if it believes a Personal Data Breach has occurred in any of the Customer's systems and provide the same information as outlined in Section 6.1 above.

6.3     In the event of any Personal Data Breach, the Parties will cooperate with each other, and take such reasonable steps as may be directed by the Customer to assist in the investigation, mitigation and remediation of the Personal Data Breach.

**7.0     Sub-Processors**

7.1     The Customer generally authorizes Bold Commerce to appoint (and to permit each Sub-Processor appointed in accordance with this Section 7 to appoint) Sub-Processors as may be required to administer and provide the Bold Commerce Services, in accordance with this Section 7 and any restrictions in the Services Agreement. An up-to-date list of vendors (including Sub-Processors) used by Bold Commerce is available on Bold Commerce's website.

7.2     Bold Commerce may continue to use those Sub-Processors already engaged by Bold Commerce as at the date of this Addendum, subject to Bold Commerce in each case meeting the obligations set out in Section 7.4.

7.3     Bold Commerce shall give the Customer prior written notice of the appointment of any new Sub-Processor, including details of the Processing to be undertaken by the Sub-Processor. If the Customer does not object to the appointment of a new Sub-Processor within 14 days of the notice described in this clause, the Customer shall be deemed to consent to the appointment of the new Sub-Processor. If the Customer objects (on reasonable grounds) to the appointment of a new Sub-Processor within 14 days of the notice, the Parties shall cooperate in good faith to determine whether it is commercially and technically practicable to accommodate the Customer's objection to the new Sub-Processor in relation to the provision of the services to the  Customer. Where such accommodation is determined to be not practicable (in the sole discretion of and as notified in writing by Bold Commerce), the Customer may terminate, on 90 days' prior written notice, that part of the services under the Services Agreement which would involve the new Sub-Processor.

7.4     Bold Commerce shall contractually require each Sub-Processor to perform substantially the same obligations as imposed upon Bold Commerce with respect to the Processing of Personal Data pursuant to this Addendum, as they apply to Processing  Personal Data provided by the Customer carried out by that Sub-Processor. Bold Commerce acknowledges and agrees that it shall remain liable to Customer for a breach of the terms of this Addendum by a Sub-Processor.

7.5     The Customer acknowledges and agrees that certain third parties which provide payment services in connection with the services to be provided by Bold Commerce pursuant to the Service Agreement act as Controllers and not as Sub-Processors of Bold Commerce. The Customer agrees and acknowledges that any transfer of Personal Data by Bold Commerce (or through Bold Commerce's services) to such third party acting in such capacity is at the instruction of the Customer (or its customers) when the Customer (or its customers) use such payment services on Bold Commerce Services.

**8.0     Assistance**

8.1     Bold Commerce shall provide the Customer with certain assistance in meeting its obligations under the GDPR including:

(a)     Provision of services to assist the Customer in viewing, editing, and deleting Personal Data of Data Subjects specific to transactions requested and executed on their store;

(b)     Custom reporting or support/customer service requests made by the Customer; and

(c)     Notification of received Data Subject requests made pursuant to the GDPR.

8.2     The Customer acknowledges that failure to meet their obligations under the GDPR may result in the immediate suspension of the services provided by Bold Commerce pursuant to the Services Agreement.

8.3     The Customer acknowledges that Bold Commerce will not provide assistance to the Customer with managing GDPR obligations that are not relevant to the services provided by Bold Commerce pursuant to the Services Agreement.

**9.0     Restricted Transfers**

9.1     Where Personal Data originating in the EEA,  UK or Switzerland is transferred to a territory that is outside the EEA, UK or Switzerland and Processed by Bold Commerce outside the EEA, UK or Switzerland, in a territory that has not been designated by the European Commission (or the relevant authority in the UK or Switzerland)  as ensuring an adequate level of protection pursuant to Data Protection Laws, Bold Commerce and the Customer agree that the transfer of such Personal Data shall be undertaken pursuant to the Standard Contractual Clauses contained in Appendixes 2 and 3 accordingly. The Parties acknowledge and agree that where Personal Data originating in the EEA, UK or Switzerland is transferred to: (a) Bold Commerce in Canada, the transfer shall be pursuant to the European Commission Decision 2002/2/EC of 20 December 2001

on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (or, in the case of the UK or Switzerland, equivalent decision as adopted under applicable law); (b) Bold Commerce, Inc. in the United States, the transfer shall be pursuant to the Standard Contractual Clauses (EEA) or the Standard Contractual Clauses UK contained in Appendixes 2 and 3. Bold Commerce shall comply with the Data Protection Laws and, as applicable, the Standard Contractual Clauses in relation to any transfers to its Sub-Processors in a territory outside the EEA, UK or Switzerland which has not been designated by the European Commission (or the relevant authority in the UK or Switzerland) as ensuring an adequate level of protection pursuant to Data Protection Laws.

9.2     If, for whatever reason, the transfers of Personal Data under clause 9.1 cease to be lawful, the Parties shall use all reasonable endeavors to promptly implement an alternative lawful transfer mechanism under the Data Protection Laws.

**10.0    Audit Rights**

10.1    Bold Commerce shall permit the Customer and/or its authorized agents to audit its records to the extent reasonably required in order to confirm that Bold Commerce is complying with its obligations under this Addendum, provided always that (a) Bold Commerce shall be given reasonable (and in any event not fewer than 6 weeks) prior written notice of any such audit, such notice shall contain a detailed description of the intended scope of such audit and the scope of such audit must be approved by Bold Commerce (such approval not to unreasonably withheld or delayed); (b) any such audit must not involve the review of any third party data, (c) any such audit shall be subject to Bold Commerce's security policies and procedures and the policies and procedures of Bold Commerce's Sub-Processors (where applicable); (d) any such audit shall be limited to one audit in any 18 months period; and (e) that the records and information accessed in connection with such audit are treated as Bold Commerce's confidential and proprietary information in accordance with the Services Agreement. Customer shall bear the costs of any such audit.

**11.0    Deletion of Personal Data**

11.1    Bold Commerce shall, promptly following receipt of written notice from the Customer, delete Personal Data from its records and, upon completion of the services described in or termination or expiration of the Services Agreement, comply with all reasonable instructions from the Customer with respect to the deletion of any remaining Personal Data.

**12.0    Liability**

12.1    Each Party is liable to the other Party for damages incurred due to the first Party's breach of this Addendum, subject to the limitations and exclusions of liability contained in the Services Agreement.

12.2    Where the Customer misrepresents or falsifies Consent of any Data Subject, it shall be fully liable for any and all damages incurred by Bold Commerce as a result of this, irrespective of any limitation or exclusion of liability contained in the Services Agreement.

**13.0    Term & Termination**

13.1    This Addendum shall take effect immediately upon signature, and remain in effect for the length of the Services Agreement, or until replaced by an updated Addendum executed by the Parties.

13.2    Bold Commerce shall, upon termination or expiration of this Addendum return or delete any Personal Data at the request of the Customer, such request to be filed with Bold Commerce within 30 days of termination or expiration of this Addendum. Bold Commerce shall confirm the return or deletion of Personal Data in response to such request in writing.

13.3    Bold Commerce will not be required to delete Personal Data where retention by Bold Commerce is mandatory to comply with applicable legal or regulatory requirements. In such case, Bold Commerce will block the Personal Data from further use, ensure the secured storage of such Personal Data, and not use such Personal Data for any other purpose than such compliance purposes. In the event deletion of any Personal Data is not practically possible due to technical limitations (taking into account the state of the art and reasonable cost associated with this deletion), the Customer acknowledges that Bold Commerce may choose to use Pseudonymisation measures, rather than delete, that certain Personal Data.

13.4    Upon expiry of applicable retention legal obligations of Bold Commerce with respect to any Personal Data, Bold Commerce shall ensure the permanent and safe deletion of all copies of such Personal Data.

## 14.0    Miscellaneous

14.1    This Addendum shall be subject to the laws agreed to be applicable and governing in the Services Agreement. In case of any conflict or dispute under this Addendum, it will be resolved solely before the competent courts as stipulated in the Services Agreement or, if applicable, in accordance with the arbitration rules specified in the Services Agreement.

14.2    No change of or amendment to this Addendum shall be valid and binding unless made in writing and agreed upon by the Parties. In case a change in Data Protection Laws makes an amendment of this Addendum necessary, the Parties will discuss and agree such required change in good faith and in writing.

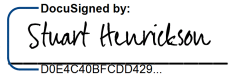**The Parties' authorized signatories have duly executed this Addendum:**

**CUSTOMER**

**BOLD INNOVATION GROUP LTD. (AND IN RELATION TO THE STANDARD CONTRACTUAL CLAUSES, BOLD COMMERCE, INC.)**

Signature: _____

Customer Legal Name: _____

Print Name: _____

Title: _____

Date: _____

DocuSigned by:

Signature: *Stuart Henrickson*
D0E4C40BFCDD429...

Print Name: Stuart Henrickson

Title: Chief Financial Officer and Corporate Secretary

Date:   18-Jan-2022

## APPENDIX 1: DETAILS OF PROCESSING OF PERSONAL DATA

This Appendix 1 includes certain details of the Processing of Personal Data as required by Article 28(3) GDPR.

### *Subject matter and duration of the Processing of Personal Data*

The subject matter and duration of the Processing of the Personal Data are set out in the Services Agreement and this Addendum.

### *The nature and purpose of the Processing of Personal Data*

Personal Data will be Processed as may be necessary to perform the services subscribed for by the Customer pursuant to the Services Agreement, and to facilitate the sales activities of the Customer through various online ecommerce platforms. This Processing may include the following:
- automated processing on behalf of the Customer and the e-commerce platforms it subscribes to or uses, including the provision and modification/formatting of Personal Data
- automated processing on behalf of the Customer to transfer Personal Data to an authorized subprocessor
- accessing Personal Data of Data Subjects specific to the Customer's transactions to assist in custom reporting or support/customer service requests made by the Customer
- facilitating the viewing, editing, and deletion of Personal Data of Data Subjects specific to the Customer by the Customer
- facilitating the intake of Personal Data, and the viewing, editing, and deletion of Personal Data specific to a Data Subject by that Data Subject
- facilitating payment transactions between Data Subject and the payment gateway(s) and sub-merchants selected by the Customer

### *The types of Personal Data to be Processed*

Name, email address, billing address and shipping address (street address, city, state/province, country, zip/postal code), phone number, user ID/credentials, transaction data, IP address/device information, and location data.

### *The categories of Data Subject to whom the Personal Data relates*

Consumers and customers of the Customer (who are natural persons), and employees, agents, advisors and consultants of the Customer (who are natural persons).

### *The obligations and rights of the Customer*

The obligations and rights of the Customer are set out in the Services Agreement and this Addendum.

## APPENDIX 2: STANDARD CONTRACTUAL CLAUSES (EEA)

**Standard Contractual Clauses**

**[Module Two: Transfer Controller to Processor]**

**[Exporter does not have a presence in the EEA]**

**[Exporter has a representative in the EEA]**

### SECTION I

*Clause 1*

***Purpose and scope***

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

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

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

have agreed to these standard contractual clauses (hereinafter: "Clauses").

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

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

*Clause 2*

***Effect and invariability of the Clauses***

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

---

[1]    Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

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

*Clause 3*

**Third-party beneficiaries**

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

(i)      Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii)     Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii)    Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv)    Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v)     Clause 13;

(vi)    Clause 15.1(c), (d) and (e);

(vii)   Clause 16(e);

(viii)  Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

*Clause 4*

**Interpretation**

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

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

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

*Clause 5*

**Hierarchy**

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

*Clause 6*

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7 – Optional [Intentionally omitted]*

~~**Docking clause**~~

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

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

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

## SECTION II – OBLIGATIONS OF THE PARTIES

*Clause 8*

***Data protection safeguards***

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

**8.1  Instructions**

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

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

**8.2  Purpose limitation**

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

**8.3  Transparency**

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

**8.4  Accuracy**

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

**8.5        Duration of processing and erasure or return of data**

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

**8.6        Security of processing**

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

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

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

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

**8.7     Sensitive data**

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

**8.8     Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

**8.9     Documentation and compliance**

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

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

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

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

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

---

[2]     The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

*Clause 9*

**Use of sub-processors**

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

*Clause 10*

**Data subject rights**

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

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

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

---

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

*Clause 11*

**Redress**

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

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

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

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

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

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

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

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

*Clause 12*

**Liability**

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

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

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

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

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

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

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

*Clause 13*

***Supervision***

**MODULE TWO: Transfer controller to processor**

(a)    The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

*Clause 14*

***Local laws and practices affecting compliance with the Clauses***

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

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

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

   (ii)    the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

---

[4]    As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal

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

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

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

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

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

*Clause 15*

**Obligations of the data importer in case of access by public authorities**

**15.1    Notification**

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

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

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

---

records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

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

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

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

## 15.2    Review of legality and data minimisation

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

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

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

## SECTION IV – FINAL PROVISIONS

### Clause 16

### Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

*Clause 17*

***Governing law***

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of **Ireland**.

*Clause 18*

***Choice of forum and jurisdiction***

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of **Ireland**.

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

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

**APPENDIX**

**EXPLANATORY NOTE:**

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

**ANNEX I**

**A. LIST OF PARTIES**

**Data exporter(s):**

[*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

**Name:**
Data Exporter is:

       (i)      The legal entity that has executed the Standard Contractual Clauses as a Data Exporter and,

      (ii)     All Affiliates (as defined in the Addendum) of the Customer established within the European Economic Area (EEA) the UK or Switzerland (or subject to the GDPR, the UK GDPR or Swiss Law) that have purchased Bold Commerce Services on the basis of one or more Order Form(s).

**Address:**

**Contact person's name, position and contact details:**

**Activities relevant to the data transferred under these Clauses:**

<mark>Signature and date:</mark>

**Role (controller/processor):**

**Data importer(s):**

[*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

**Name:** Bold Commerce, Inc.

**Address:** 600 Congress Avenue, Austin, TX, USA, 78701

**Contact person's name, position and contact details:** Rene Mendizabal, Privacy Officer, privacy@boldcommerce.com

**Activities relevant to the data transferred under these Clauses:**

- Receiving data, including collection, accessing, retrieval, recording, and data entry

- Holding data, including storage, organization and structuring

- Protecting data, including restricting, encrypting, and security testing

- Sharing data, including disclosure, dissemination, allowing access or otherwise making available

**Signature and date:** *Stuart Henrickson*   18-Jan-2022
DocuSigned by:
D0E4C40BFCDD429...
**Role (controller/processor):** Processor

### B. DESCRIPTION OF TRANSFER

*Subject matter and duration of the Processing of Personal Data*

The subject matter and duration of the Processing of the Personal Data are set out in the Services Agreement and this Addendum.

*The obligations and rights of the Customer*

The obligations and rights of the Customer are set out in the Services Agreement and this Addendum.

*Categories of data subjects whose personal data is transferred*

Consumers and customers of the Customer (who are natural persons), and employees, agents, advisors and consultants of the Customer (who are natural persons).

*Categories of personal data transferred*

Name, email address, billing address and shipping address (street address, city, state/province, country, zip/postal code), phone number, user ID/credentials, transaction data, IP address/device information, and location data.

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

*N/A*

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

Continous basis

*Nature of the processing*

Personal Data will be Processed as may be necessary to perform the services subscribed for by the Customer pursuant to the Services Agreement, and to facilitate the sales activities of the Customer through various online ecommerce platforms. This Processing may include the following:

- Automated processing on behalf of the Customer and the e-commerce platforms it subscribes to or uses, including the provision and modification/formatting of Personal Data
- Automated processing on behalf of the Customer to transfer Personal Data to an authorized sub-processor

- Accessing Personal Data of Data Subjects specific to the Customer's transactions to assist in custom reporting or support/customer service requests made by the Customer
- Facilitating the viewing, editing, and deletion of Personal Data of Data Subjects specific to the Customer by the Customer
- Facilitating the intake of Personal Data, and the viewing, editing, and deletion of Personal Data specific to a Data Subject by that Data Subject
- Facilitating payment transactions between Data Subject and the payment gateway(s) and sub-merchants selected by the Customer

*Purpose(s) of the data transfer and further processing*

Personal Data will be Processed as may be necessary to perform the services subscribed for by the Customer pursuant to the Services Agreement, and to facilitate the sales activities of the Customer through various online ecommerce platforms.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

- As defined on Bold's Records Retention Policy and Records Retention Schedules

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

- As defined on Bold's Records Retention Policy and Records Retention Schedules

## C. COMPETENT SUPERVISORY AUTHORITY

***Identify the competent supervisory authority/ies in accordance with Clause 13***

[Data exporter to complete this information]

Swiss Federal Data Protection and Information Commissioner (**FDPIC**) will be the supervisory authority for data transfers covered by the Swiss Federal Act of 19 June 1992 on Data Protection.

## ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

**EXPLANATORY NOTE:**

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

- Data encryption
- Secure storage
- Access control
- Shredding and/or deletion of extraneous records
- Clean desk policy
- Password security
- Regular penetration testing
- Firewalls

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

- Data encryption
- Secure storage
- Access control
- Shredding and/or deletion of extraneous records
- Clean desk policy
- Password security
- Regular penetration testing
- Firewalls

## ANNEX III:
## EXPORTING OF PERSONAL DATA FROM SWITZERLAND TO A COUNTRY WITH AN INADEQUATE LEVEL OF DATA PROTECTION

1. Where the performance of this agreement requires the export of personal data from Switzerland to a country with an inadequate level of data protection, the Standard Contractual Clauses (EU) contained in the Appendix 2 of this agreement shall be interpreted as follows:

   a. The term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c.
   b. References to the GDPR should be understood as references to the Swiss Federal Act of 19 June 1992 on Data Protection (FADP) insofar as the data transfers are subject to the FADP.
   c. The Standard Contractual Clauses also protect the data from legal entities until the entry into force of the revised FADP.
   d. Annex I.C. designates the Swiss Federal Data Protection and Information Commissioner (**FDPIC**) as the supervisory authority for data transfers covered by the FADP

## APPENDIX 3: STANDARD CONTRACTUAL CLAUSES (UK)

The standard contractual clauses for international transfers from controllers to processors

| | | Non-legally binding guidance |
|---|---|---|
| | | This column does not form part of the standard contractual clauses, and is not legally binding on either party |
| | | |
| **Parties** | | |
| Name of the data exporting organisation: | Click here to enter text. | This is the sender of the restricted transfer of personal data (referred to as the exporter). Insert the full legal name: • If a sole trader, his/her full name. • If a company or limited liability partnership – as formally registered. • If a partnership as set out in Partnership Deed. If an unincorporated association, check the establishing document, as to who should enter into this contract. |
| Address | Click here to enter text. Country: Click here to enter text. | This is the contact address for the exporter. It may be the registered address but does not need to be. You must include the country. |
| Telephone | Click here to enter text. | This can be the exporter's general contact telephone number. |
| Fax | Click here to enter text. | This can be the exporter's general contact fax number. Leave this blank if you do not have a fax. |
| Email | Click here to enter text. | This can be the exporter's general contact email address |
| Other information needed to identify the organisation | Click here to enter text. | For UK companies and limited liability partnerships it is helpful to include the following: A company/limited liability partnership (delete as appropriate) registered in England and Wales/Scotland/Northern Ireland (delete as appropriate). Company number: insert number. For companies outside the UK, if possible it is helpful to include the registration number and country of incorporation. A company number is useful as it can help identify a company even if it has changed its name and address. |
| | (the data **exporter**") | |
| | And | |
| Name of the data importing organisation: | **Bold Commerce, Inc** | This is the receiver of the restricted transfer of personal data (referred to as the importer). Insert the full legal name: • If a sole trader, his/her full name. • If a company or limited liability partnership – as formally registered. • If a partnership as set out in Partnership Deed. • If an unincorporated association, check the establishing document, as to who should enter into this contract. |
| Address | 600 Congress Avenue, Austin, Texas, USA, 78701 Country: United States | This is the contact address for the importer. It may be the registered address but does not need to be. You must include the country. |
| Telephone | Click here to enter text. | This can be the importer's general contact telephone number. |
| Fax | Click here to enter text. | This can be the importer's general contact fax number. Leave this blank if you do not have a fax. |

| Email | **privacy@boldcommerce.com** | This can be the importer's general contact email address |
|---|---|---|
| Other information needed to identify the organisation | Click here to enter text. | For UK companies and limited liability partnerships it is helpful to include the following:<br><br>A company/limited liability partnership (delete as appropriate) registered in England and Wales/Scotland/Northern Ireland (delete as appropriate).<br><br>Company number: insert number<br><br>For companies outside the UK, if possible it is helpful to include the registration number and country of incorporation.<br><br>A company number is useful as it can help identify a company even if it has changed its name and address. |
| | (the data **importer**") | |
| **1. Definitions** | For the purposes of the Clauses:<br><br>(a)'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'Commissioner' shall have the same meaning as in the UK GDPR; | A brief overview of these definitions are:<br><br>"Personal data"<br>Information relating to an identified or identifiable natural person.<br><br>"Special categories of data"<br>Personal data which relates to an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.<br><br>"Process/processing"<br>In practice means anything which can be done to data, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.<br><br>"Controller"<br>A natural or legal person which decides the purposes and means of processing data<br><br>"Processor"<br>A natural or legal person which is responsible for processing personal data on behalf of a controller<br><br>"Data subject"<br>The individual that personal data relates to.<br><br>"The Commissioner"<br>The Information Commissioner, as the UK's independent data protection authority, which we refer to as the 'ICO'. |
| | (b) 'the data exporter' means the controller who transfers the personal data; | This is the sender/exporter of the personal data, set out on page 1. |
| | (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf | This is the receiver/importer of the personal data, set out on page 3.<br><br>The definition clarifies that the importer should not be in a country covered by UK "adequacy regulations".<br><br>These are UK regulations confirming that the legal framework in a country (or territory or sector) provides an adequate level of data |

| | |
|---|---|
| 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 covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018; | protection for personal data. Currently, it includes all EEA countries and all countries (territories or sectors) covered by a European Commission "adequacy decision"<br><br>You do not need to use the standard contractual clauses if the importer is covered by UK adequacy regulations. |
| (d) 'the 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; | This is a sub-contractor of the processor, to which the processor has delegated some of its personal data processing services. |
| (e) '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 UK; | "Applicable data protection law" means the data protection law of the UK which is the UK GDPR and the Data Protection Act 2018 ("DPA 2018"). |
| (f) '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 | This definition is aligned with UK GDPR Art 32, which places obligations on both controllers and processors to keep personal data secure.<br><br>In brief, this requires security measures that involve policies, processes and people as well as technology. This usually means that:<br>• You consider things like risk analysis, organisational policies and physical and technical measures.<br>• You take into account additional requirements about the security of your processing. |

| | | |
|---|---|---|
| | access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. | • You consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.<br>• Where appropriate, you should look to use measures such as pseudonymisation and encryption.<br>• Your measures must ensure the confidentiality, integrity and availability of your systems and services and the personal data you process within them.<br>• The measures must also enable you to restore access to and availability of personal data in a timely manner in the event of a physical or technical incident.<br>• You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures regularly (such as pen testing and testing application security), and undertake any required improvements. |
| **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. | You must fill in Appendix 1 with the details of the restricted transfer (see below).<br><br>Clause 2 flags that if "special categories of personal data" are being transferred these should be set out, as they receive a higher standard of protection in data protection law. |
| **3. Third-party beneficiary clause** | | Clause 3 sets out the rights of data subjects to enforce certain provisions in the standard contractual clauses against the importer and exporter.<br><br>Data subjects do not sign up to the standard contractual clauses, but they can enforce compliance with particular clauses which are intended to benefit them. The clauses which can be enforced by a data subject are set out below.<br><br>If a data subject wishes to bring a claim for non-compliance with the standard contractual clauses, it must first try to bring the claim against the exporter.<br><br>If it is not possible to bring a claim against the exporter, the data subject can try to bring a claim against the importer (see Cl 3(2))<br><br>If it is not possible to bring a claim against the importer, the data subject can try to bring a claim against a sub-processor (if there is one) (see Cl 3(3)). |
| | 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. | Data subjects can enforce the clauses listed directly against the exporter. |
| | | Data subject enforcement against:<br>☑ Exporter<br>(if that is not possible:)<br>☑ Importer<br>(if that is not possible:)<br>☑ Sub-processor |
| | The data subject can enforce against the data | Data subjects can enforce the clauses listed directly against the importer, but only where: |

| | 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. | • the exporter has "factually disappeared" (for example, it is not contactable or traceable) OR it no longer legally exists (for example, it is a company which has been dissolved); and <br>• there is no entity which has taken over <u>all</u> of the exporter's obligations. |
|---|---|---|
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | 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 | Data subjects can enforce the clauses set out listed directly against the sub-processor if:<br>• both the exporter and importer have either "factually disappeared" (for example, neither is contactable or traceable) OR no longer legally exist (for example: a company which has been dissolved); and<br>• there is no entity which has taken on <u>all</u> of the exporter's obligations. |

| | | |
|---|---|---|
| | operations under the Clauses. | |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | 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. | This clause prevents the exporter and importer objecting to data subjects being represented by associations or other bodies (eg interest or campaign groups). |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| **4. Obligations of the data exporter** | The data exporter agrees and warrants: | Clause 4 sets out the general commitments which the exporter provides in relation to the data.<br><br>These commitments are "warranties", which are promises given in a contract.<br><br>If the exporter does not comply with a warranty, this may lead to a claim from the importer for damages.<br><br>If the exporter does not comply with certain obligations, this may lead to a claim from data subjects. We have shown below where a data subject can take such action in relation to a clause. These are also set out in Clause 3 above. |
| | 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 Commissioner) and does not violate the applicable data protection law; | The exporter of the data must make sure that it has complied with the UK GDPR and DPA 2018 (and all other UK laws which apply to it), in relation to its collection, use and transfer of the personal data being sent under the standard contractual clauses.<br><br>The clause refers to notifying the ICO about processing activities. However, exporters in the UK no longer need to notify the ICO of their processing of personal data. |

| | | |
|---|---|---|
| | 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; | The exporter must only instruct the importer to process the data on the exporter's behalf (i.e. for the purposes instructed by the exporter).<br><br>The instructions must also be:<br>• in accordance with the UK GDPR and the DPA 2018; and<br>• in accordance with the standard contractual clauses.<br>This means that the exporter cannot instruct the importer to do something which is not permitted by the UK GDPR and DPA 18, or by the standard contractual clauses. |
| | | Data subject enforcement against:<br>☑ Exporter |
| | that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract; | The exporter must ensure that the importer provides sufficient guarantees in relation to the security measures set out by the parties in Appendix 2.<br><br>In practice, ensuring that the importer provides sufficient guarantees is likely to involve the exporter carrying out due diligence on the importer before it selects it as a processor. This might include:<br>• asking questions about the importer's data protection practices;<br>• reviewing its security measures;<br>• reviewing its internal data protection policies; and<br>• asking questions about any previous data security incidents. |
| | | Data subject enforcement against:<br>☑ Exporter |
| | 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; | This clause requires the exporter to have assessed the importer's security measures, both technical and organisational (which includes policies, processes and people).<br><br>The exporter must be satisfied that these security measures offer appropriate protection for the data being transferred, to protect it against it being destroyed, lost, altered or disclosed, or accessed by unauthorised persons.<br>The UK GDPR and the standard contractual clauses do not set any specific mandatory security measures.<br>It is for the exporter to assess what measures are appropriate in the circumstances, taking into account:<br>• the nature of the data;<br>• the nature of the technology used to process the data;<br>• the cost of implementing any particular measures; and<br>• the risks that could arise from any accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access to the personal data.<br>The parties should keep the measures under review and be aware that they may need to change or update them over time as new technology becomes available, or if the risks of the processing change. |
| | | Data subject enforcement against:<br>☑ Exporter |

| | that it will ensure compliance with the security measures; | This clause makes the exporter responsible for ensuring that the importer complies with the security measures set out in Appendix 2.<br><br>This is an on-going obligation which lasts for the duration of the processing by the importer.<br><br>This means that the exporter should take steps throughout the life of the contract to make sure that the importer is complying with the measures. This could be by asking questions to the importer or by audits of the importer on a regular basis (such as annually). |
|---|---|---|
| | | Data subject enforcement against:<br>☑ Exporter |
| | 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 covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018; | This clause only applies where special categories of data are transferred to the importer.<br><br>In that case, the exporter must tell data subjects that their data has been transferred outside the UK to a country not covered by UK adequacy regulations. |
| | | Data subject enforcement against:<br>☑ Exporter |
| | to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension; | This clause relates to circumstances in which the exporter has received one (or both) of the following notifications from the importer.<br>- **A notification under clause 5(b):** that the laws which apply to the importer have changed and this is likely to have a substantial adverse effect on the importer's obligations under the standard contractual clauses.<br>- **A notification under clause 8(3):** telling the exporter about any laws applicable to the importer which prevent an audit by the ICO of the importer or any sub-processor.<br>If the exporter receives such a notification but still plans to continue the transfer of data to the importer or (if it has stopped transferring personal data) to lift a suspension, it must forward the notification to ICO).<br><br>This is so that the ICO can decide whether to audit the importer to ensure that the personal data is adequately protected. |
| | | Data subject enforcement against:<br>☑ Exporter |
| | 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 | The exporter must provide copies of the following documents/ information to data subjects who request them:<br>• the standard contractual clauses (excluding Appendix 2);<br>• a summary description of the security measures in Appendix 2; and<br>• any contract for sub-processing services which has to be made in accordance with the standard contractual clauses (see clause 11 below which covers using a sub-processor). |

| | | |
|---|---|---|
| | 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; | • The exporter can remove commercial information before disclosing the standard contractual clauses and any sub-processing contract to a data subject. |
| | | Data subject enforcement:<br>☑ Exporter |
| | 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; | The exporter must make sure that:<br>• any sub-processing is carried out in accordance with the requirements of clause 11; and<br>• any sub-processor provides at least the same level of data protection and rights of data subjects as the importer is required to provide under the standard contractual clauses. |
| | | Data subject enforcement against:<br>☑ Exporter |
| | that it will ensure compliance with Clause 4(a) to (i). | This clause requires the exporter to ensure its own compliance with clauses 4(a) to 4(i), set out above.<br><br>In practice, this means that the exporter will need to make sure its employees, contractors and agents comply with clauses 4(a) to 4(i). |
| **5. Obligations of the data importer** | The data importer agrees and warrants: | Clause 5 sets out the general commitments which the importer gives in relation to the data.<br><br>These commitments are "warranties", which are promises given in a contract.<br><br>If the importer does not comply with a warranty, this may lead to a claim from the exporter for damages against the importer.<br><br>In addition, if the importer does not comply with certain obligations, this may lead to a claim from data subjects.<br><br>We have indicated below where a data subject can take such action in relation to a clause. These are also set out in Clause 3 above.<br><br>The obligations in Clause 5 are intended to make sure that the importer, who is not subject to the UK GDPR, provides at least the same level of protection for the personal data as required under the UK GDPR. |
| | 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 | The importer must process the data:<br>• only on behalf of the exporter; and<br>• in accordance with the exporter's instructions.<br><br>• If the importer cannot do this, it must promptly tell the exporter. Following this, the exporter can suspend the transfer of data to the importer and/or the exporter can terminate the contract. |

| | | |
|---|---|---|
| | 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; | |
| | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor | |
| | 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; | This clause requires the importer to consider the laws that apply to it and whether any of those laws will prevent it from meeting the exporter's instructions and complying with its obligations under the standard contractual clauses.<br><br>If any of the laws which apply to the importer change – and these changes are likely to have a substantial adverse effect on the promises and obligations set out in the standard contractual clauses – the importer must notify the exporter as soon as it becomes aware of the changes.<br><br>A "substantial adverse effect" would be any legal requirement on the importer which might prevent the importer from complying with the standard contractual clauses.<br><br>In these circumstances, the exporter can stop the transfer of data to the importer and/or terminate the contract. |
| | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor | |
| | that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred; | The importer must put in place the security measures contained in Appendix 2 before it starts processing the data. This effectively means that the security measures must be place before the data is transferred to the importer.<br><br>The UK GDPR or the standard contractual clauses do not set any mandatory security measures. It is for the exporter to assess what is appropriate in the circumstances.<br><br>When deciding what security measures are appropriate, the receiver should think about the type of data (eg how sensitive it is), the type of processing carried out (eg how intrusive it is) and the likely harm which could come to data subjects if the data were lost, stolen or accessed by an unauthorised person. |

| | | |
|---|---|---|
| | | Further guidance:<br>• ICO: A Practical Guide to IT Security<br>• NCSC: Cyber Security: Small Business Guide<br>• NCSC: Cyber Essentials Scheme |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | that it will promptly notify the data exporter about:<br><br>(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 unauthorised access; and (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so; | The importer must promptly tell the exporter about:<br>• any legally binding request for disclosure of the personal data it receives from a law enforcement agency (unless it is prohibited by law from telling the exporter);<br>• any accidental, unlawful or unauthorised access to the data; and<br>• any request the importer receives directly from a data subject. The importer must not respond to a request from a data subject unless the exporter authorises it to do so. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | 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 Commissioner with regard to the processing of the data transferred; | The importer must respond promptly to any questions from the exporter about the importer's processing of the data.<br><br>The importer must also follow the advice of the ICO about the processing of the personal data transferred, as the restricted transfer is from an exporter in the UK. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |

| 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 Commissioner; | If the exporter requests, the importer must allow the exporter to carry out an audit of the facilities it uses to process the personal data transferred.<br><br>Audits can be carried out by:<br>• the exporter itself; or<br>• third party auditors appointed by the exporter. These auditors must be independent and have appropriate professional qualifications. They must also be subject to confidentiality obligations in relation to the data.<br>The appointment of third party auditors does not currently require agreement by the ICO. |
|---|---|
| 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; | The importer must provide copies of the following documents/information to data subjects who request them:<br>• the standard contractual clauses (excluding Appendix 2);<br>• a summary description of the security measures in Appendix 2; and<br>• any existing contract for sub-processing.<br>• The importer can remove commercial information from the sub-processing contracts and the standard contractual clauses before disclosing them to a data subject. |
| | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| that, in the event of sub-processing, it has previously informed the data exporter and | The importer can only appoint sub-processors to process the personal data if it has told the exporter about this – and the exporter has consented in writing beforehand to this appointment. |

| | | |
|---|---|---|
| | obtained its prior written consent; | • The authorisation required for appointing sub-processors should be set out in the main contract between the exporter and the importer (under UK GDPR rules on controller-processor contracts). |
| | | Data subject enforcement:<br>☑ Exporter<br>☑ Importer<br>☑ Sub-processor |
| | that the processing services by the sub-processor will be carried out in accordance with Clause 11; | • The importer must make sure that its sub-processors process the personal data in accordance with clause 11. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter. | • The importer must promptly provide to the exporter a copy of all sub-processing agreements it enters into under the standard contractual clauses. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| **6. Liability** | | Clause 6 sets out which parties will be liable for breaches of the standard contractual clauses. It also sets out data subjects' rights to enforce compliance with the standard contractual clauses by both the exporter and importer. |
| | 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. | • If a data subject suffers damage due to a breach of clauses 3 or 11 by any of the exporter, the importer or a sub-processor, the exporter is responsible in the first instance for compensating the data subject. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | If a data subject is not able to bring a claim for compensation in | As set out against clause 3, above, if there has been a breach of the clauses set out in clauses 3 or 11 by the exporter, importer or any sub-processor, the data subject should try to bring a claim against the exporter first. |

| | | |
|---|---|---|
| | 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.<br><br>The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities. | If the data subject cannot bring a claim against the exporter because the exporter has factually disappeared, no longer exists in law, or is insolvent, the data subject can bring a claim against the importer.<br><br>This does not apply if a successor entity has taken on all the legal obligations of the exporter by contract or by operation of law. In that case, the data subject should bring a claim against the exporter's successor. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | 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 | As set out in clause 3, if there has been a breach by a sub-processor of clause 3 or 11, the data subject should try to bring a claim first against the exporter and then the importer.<br><br>This clause explains that: if the data subject cannot bring a claim against the exporter or the importer because they have factually disappeared, no longer exist in law or are insolvent, the sub-processor agrees that the data subject can bring a claim against it for the sub-processor's own breaches.<br><br>This does not apply if a successor entity has taken on all the legal obligations of the exporter or importer by contract or operation of law. In this case, the data subject should bring a claim against the successor. |

| | | |
|---|---|---|
| | 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. | |
| **7. Mediation and jurisdiction** | | Clause 7 relates to circumstances in which a data subject can bring a claim against the importer for breach of the standard contractual clauses. |
| | 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:<br><br>(a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;<br>(b) to refer the dispute to the UK courts. | If a data subject decides to bring a claim against the importer for breach of the standard contractual clauses, the data subject can choose to either:<br>• refer disputes to mediation by an independent person or the ICO; or<br>• bring a claim in the courts of the UK.<br>• The importer must accept the data subject's decision. |
| | | Data subject enforcement against:<br>☑ Exporter |

| | | |
|---|---|---|
| | | If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | 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. | • This is an acknowledgement by the exporter and importer that: regardless of whether the data subject chooses mediation or a court action, the data subject can still take advantage of any other remedies which are available to them under national or international law. |
| | | Data subject enforcement:<br>☑ Exporter<br>☑ Importer<br>☑ Sub-processor |
| **8. Cooperation with supervisory authorities** | The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law. | The exporter must give a copy of the standard contractual clauses to the ICO if the ICO requests it (or if it is required under applicable data protection law). |
| | The parties agree that the Commissioner 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. | The ICO can audit the importer and any sub-processor, in the same way as it could audit the exporter.<br>• |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | 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 | The importer must tell the exporter about any laws which apply to the importer or any of its sub-processors which would prevent the importer/sub-processor from being audited by the ICO.<br><br>If there are such laws, the exporter can suspend the transfer of data to the importer and/or terminate the contract. |

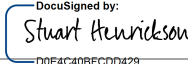| | | |
|---|---|---|
| | paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b). | |
| **9. Governing law** | The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely Click here to enter text. | The standard contractual clauses are governed by the law of the UK country of the exporter.<br><br>→ **ACTION**: Fill out this section with the law of the UK where the exporter is established.<br><br>i.e. choose one of "England and Wales", "Scotland" or "Northern Ireland". |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| **10. Variation of the contract** | The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause. | The parties must not amend the standard contractual clauses although:<br><br>- they must fill in the Appendices and governing law in clauses 9 and 11;<br><br>- they may make changes which are only to make the Clauses make sense in a UK context (as permitted by Paragraph 7(3) & (4) of Schedule 21 DPA 2018).<br><br>- they may add commercial clauses which don't contradict the standard contractual clauses. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| **11. Sub-processing** | | This clause covers the use of sub-processors by the importer.<br><br>• A sub-processor is a processor engaged by the importer to carry out processing activities on behalf of the exporter. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the | The importer can only use a sub-processor if the exporter agrees to this in writing beforehand.<br><br>There should be rules in the main controller-processor contract regarding how the importer appoints a sub-processor, to meet the requirements of the UK GDPR. |

| | | |
|---|---|---|
| | 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. | If the importer uses a sub-processor, it must enter into a written agreement with the sub-processor. This written agreement must include the same obligations for the sub-processor as those which apply to the importer under the standard contractual clauses.

In practice, many importers meet this requirement by having the sub-processor co-sign the standard contractual clauses between the exporter and the importer.

Alternatively, many importers meet this requirement by entering into a duplicate with the sub-processor (i.e. entering into a copy of the same standard contractual clauses as the importer and exporter have signed).

• If a sub-processor does not comply with its equivalent contractual obligations, the importer remains liable to the exporter for this. It is therefore in the importer's interests to choose its sub-processors carefully. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | 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 | The contract between the importer and the sub-processor must include rights for data subjects to bring claims against the sub-processor if:

• both the exporter and importer no longer exist in law (eg a company which has been dissolved), have factually disappeared (for example, they are uncontactable or traceable) or are insolvent; and<br>• no entity has taken on all of the exporter's obligations (in which case the data subject may bring action against that successor entity).<br>• Claims by data subjects against a sub-processor are limited to damages caused by sub-processor's own processing activities. |

| | | |
|---|---|---|
| | 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. | |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established. | The agreement between the importer and the sub-processor must be governed by the same law as the standard contractual clauses, set out in Clause 9 above.<br><br>• |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | 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 Commissioner. | The exporter must keep a list of sub-processing agreements which the importer has:<br>• entered into in relation to the data which is being transferred under the standard contractual clauses; and<br>• has told the exporter about.<br>The exporter must update this list at least once a year.<br><br>The exporter must provide this to the ICO if the ICO requests it. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| **12. Obligation after termination** | | • Clause 12 sets out obligations under the standard contractual clauses which the parties must still comply with even after the |

| | | |
|---|---|---|
| | | contract has ended, and the importer is no longer providing the data processing services. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | 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. | On termination of the data processing services, the importer and all sub-processors must either return all the personal data to the exporter or destroy it.<br><br>It is up to the exporter to choose whether the data should be returned or destroyed.<br><br>If the exporter chooses for the importer and sub-processors to destroy the data, the importer and sub-processors must confirm in writing to the exporter that they have done this.<br><br>If laws which apply to the importer/sub-processor mean that they cannot destroy or return the data, they must keep the data confidential and not process it in any other way. The importer is responsible for making sure its sub-processors do this. |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| | The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for | The exporter can audit the importer and the sub-processor to check that they have destroyed the personal data and/or kept it confidential after its processing activity for the exporter has come to an end.<br><br>• The ICO can also audit the importer and the sub-processor to check that they have destroyed this data after its processing activity for the exporter has come to an end. |

| | | |
|---|---|---|
| | an audit of the measures referred to in paragraph 1. | |
| | | Data subject enforcement against:<br>☑ Exporter<br>If that is not possible:<br>☑ Importer<br>If that is not possible:<br>☑ Sub-processor |
| **Additional commercial clauses** | The parties are able to add additional commercial clauses.<br><br>When including additional commercial clauses, the parties should ensure that these clauses do not in any way:<br>• overlap with or contradict the standard contractual clauses;<br>• reduce the level of protection which the data importer is required to provide for the personal data; or<br>• reduce the rights of data subjects, or make it any more difficult for them to exercise their rights. | You may add any additional commercial clauses to the standard contractual clauses.<br><br>You do not need to add any of these clauses in order to comply with the UK GDPR rules on restricted transfers.<br><br>When including additional commercial clauses, the parties should ensure that these clauses do not in any way:<br>• overlap with or contradict the standard contractual clauses;<br>• reduce the level of protection which the data importer is required to provide for the personal data; or<br>• reduce the rights of data subjects or make it more difficult for them to exercise their rights.<br>We do not recommend including terms required under UK GDPR for a controller-processor contract in the standard contractual clauses. In nearly all cases it is better to have those in a separate agreement.<br><br>If you are unsure whether or not you can add a particular additional clause or not, you should consider adding it to your main controller – processor agreement instead. |
| **Indemnification** | Please click in the box if you wish to include the following optional clause:<br>    X **Include**<br><br>Liability<br>Subject to the limitations and exclusions of liability contained in the Services Agreement, the parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the | This indemnification clause is included an example of an additional clause which you could include.<br><br>This example is optional – you do not need to include it, and you can choose to add other additional commercial clauses instead of, or in addition to, this example. You can also amend this example.<br><br>The clause is a mutual indemnity:<br>• the importer indemnifies the exporter; and<br>• the exporter indemnifies the importer;<br>if either of them is in breach of the standard contractual clauses.<br><br>In this context, an "indemnity" means that the party in breach has to fully compensate the other for its losses which arise from its breach. This may be more than just a standard claim for breach of contract, where damages can be claimed.<br><br>This clause provides a route for an innocent party to claim back from the other any compensation it has had to pay to a data subject under the standard contractual clauses, arising from a breach by that other party. |

| | first party for any cost, charge, damages, expenses or loss it has incurred.<br><br>Indemnification is contingent upon:<br><br>(a) the data exporter promptly notifying the data importer of a claim; and<br>(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim. | This example indemnity is wider than that, and provides additional compensation for any breach of the standard contractual clauses.<br><br>Indemnities are often dealt with in the main controller – processor contract between the parties. |
|---|---|---|
| **Priority of standard contractual clauses** | Please click in the box if you wish to include the following optional clause:<br><br>X **Include**<br><br>The Standard Contractual Clauses take priority over any other agreement between the parties, whether entered into before or after the date these Clauses are entered into.<br><br>Unless the Clauses are expressly referred to and expressly amended, the parties do not intend that any other agreement entered into by the parties, before or after the date the Clauses are entered into, will amend the terms or the effects of the Clauses, or limit any liability under the Clauses, and no term of any such other agreement should be read or interpreted as having that effect. | This clause is provided as it may also be helpful to you.<br><br>Please review it carefully and only include it if you think it is appropriate for your circumstances.<br><br>The intended effect of the clause is to make sure that you and the other party do not inadvertently amend the standard contractual clauses or limit your liability. If you did, then you would risk not being able to rely on the standard contractual clauses for compliance with the UK GDPR rules on restricted transfers.<br><br>The clause allows you the freedom to amend the standard contractual clauses, but only if you expressly refer to them.<br><br>If you are going to amend the standard contractual clauses, we would always recommend you seek professional legal advice.<br><br>Any amendment runs the risk that the standard contractual clauses will not comply with the UK GDPR rules on restricted transfers. |
| | | |
| On behalf of the data exporter:<br>Name (written out in full):<br>Click here to enter text. | | → **ACTION**: The exporter should fill in this section with the:<br>• Full name of the person signing. This must be a person who is authorised to enter into contracts on behalf of the exporter. |

| | |
|---|---|
| Position:<br>Click here to enter text.<br>Address:<br>Click here to enter text.<br>Other information necessary in order for the contract to be binding (if any): Click here to enter text.<br>Signature:<br>Click here to enter text. | • Their position.<br>• Their business addresses.<br>And sign where indicated. |
| On behalf of the data importer:<br>Name (written out in full):<br>**Stuart Henrickson**<br>Position:<br>Secretary, Treasurer<br>Address:<br>**600 Congress Avenue, Austin, TX, USA, 78701**<br>Other information necessary in order for the contract to be binding (if any):<br>Signature: *DocuSigned by:*<br>*Stuart Henrickson*<br>D0E4C40BFCDD429... | → **ACTION**: The importer should fill in this section with the:<br>• Full name of the person signing. This must be a person who is authorised to enter into contracts on behalf of the importer.<br>• Their position.<br>• Their business addresses.<br>• And sign where indicated. |
| Date of the Standard Contractual Clauses:<br><br>Click here to enter text. | Do not date the standard contractual clauses until both the exporter and importer have signed.<br>It can be the date of the last signature, or a later date if that is agreed by the exporter and importer. |

1

| | **Non-legally binding guidance** |
|---|---|
| Appendix 1 | |
| This Appendix forms part of the Clauses and must be completed and signed by the parties. | → **ACTION**: This Appendix must be appropriately completed for the standard contractual clauses to be an appropriate safeguard and allow restricted transfers of personal data under the UK GDPR.<br><br>Currently, the UK does not require any additional information to be included in the Appendix.<br><br>Instructions for using the checklists:<br>To help you completing this Appendix, we have provided optional checklists. These are just suggestions. You do not need to use the checklists at all.<br><br>You can also amend the contents of any category, as you consider best reflects the international transfer of personal data, including to add specific details. If you do not fit into any of these types, you may add your own description at the endof the checklist. |
| **Data exporter** | |
| The data exporter is (please specify briefly your activities relevant to the transfer):<br><br>*Please select one option:* | → **ACTION**: Set out the exporter's type of business and its activities relevant to the restricted transfer.<br><br>You have two options:<br><br>Option 1. You may set this out in your own words.  As a suggestion, you could use the following form: |

☐ <u>Option 1</u>: The data exporter is (please specify briefly your activities relevant to the transfer):

☐ <u>Option 2</u>: The following checklist and other details set out, in brief, what the data exporter is and its activities relevant to the transfer:

**The data exporter's business or organisation type is:**

☐ Central government

☐ Charitable and voluntary

☐ Education and childcare

☐ Finance, insurance and credit

☐ General business

☐ Health

☐ IT, digital, technology and telecoms

☐ Justice and policing

☐ Land and property services

☐ Legal and professional advisers

☐ Local government

☐ Marketing and research

☐ Media

☐ Membership association

☐ Political

☐ Regulators

☐ Religious

☐ Research

☐ Retail and manufacture

☐ Social care

☐ Trade, employer associations, and professional bodies

☐ Traders in personal data

☐ Transport and leisure

☐ Utilities and natural resources

☐ Other – Please add details:


**The data exporter is using the personal data which is being transferred for the following purposes or activities:**
The data exporter is using the personal data which is being transferred for the following purposes or activities:

---

**The data exporter is:** insert description of importer.
**The data exporter's activities which are relevant to the restricted transfer are:** add activities.

For example:
"The data exporter is a UK-based supplier of home office equipment and is contracting with the importer for it to provide a software solution for managing the exporter's customer database".

You should also have a controller-processor contract in place. If so, you may be able to re-use a description of the exporter's activities as set out in that contract.

<u>Option 2</u>: you may find it easier to use the checklists provided.

<u>Instructions</u>:
Step 1: Think about the exporter's <u>type of business or organisation</u> and click in the box next to the appropriate category, making any appropriate amendments or adding specific detail.

Step 2: Think about <u>why</u> the exporter is using the personal data to be transferred and why it is making the transfer. Click in the box next to all of the activities which apply, making appropriate amendments or adding specific details. You can click "other" and add your own description at the end.

---

Standard business activities, which apply to most businesses and organisations

☐ Staff administration, including permanent and temporary staff, including appointment or removals, pay, discipline; superannuation, work management, and other personnel matters in relation to the data exporter's staff.

☐ Advertising, marketing and public relations of the data exporter's own business or activity, goods or services.

☐ Accounts and records, including

• keeping accounts relating to the data exporter's business or activity;
• deciding whether to accept any person or organisation as a customer;
• keeping records of purchases, sales or other transactions, including payments, deliveries or services provided by the data exporter or to the data exporter;
• keeping customer records
• records for making financial or management forecasts; and
• other general record keeping and information management.
Other activities:

☐ Accounting and auditing services

☐ Administration of justice, including internal administration and management of courts of law, or tribunals and discharge of court business.

☐ Administration of membership or supporter records.

☐ Advertising, marketing and public relations for others, including public relations work, advertising and marketing, host mailings for other organisations, and list broking.

☐ Assessment and collection of taxes, duties, levies and other revenue

☐ Benefits, welfare, grants and loans administration

☐ Canvassing, seeking and maintaining political support amongst the electorate.

☐ Constituency casework on behalf of individual constituents by elected representatives.

☐ Consultancy and advisory services, including giving advice or rendering professional services, and the provision of services of an advisory, consultancy or intermediary nature.

☐ Credit referencing, including the provision of information by credit reference agencies relating to the financial status of individuals or organisations on behalf of other organisations

☐ Data analytics, including profiling

☐ Debt administration and factoring, including the tracing of consumer and commercial debtors and the collection on behalf of creditors, and the purchasing of consumer or trade debts from business, including rentals and instalment credit payments.

☐ Education, including the provision of education or training as a primary function or as a business activity.

☐ Financial services and advice including the provision of services as an intermediary in respect of any financial transactions including mortgage and insurance broking

☐ Fundraising in support of the objectives of the data exporter

☐ Health administration and services, including the provision and administration of patient care.

☐ Information and databank administration, including the maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.

☐ Insurance administration including the administration of life, health, pensions, property, motor and other insurance business by an insurance firm, an insurance intermediary or consultant

☐ IT, digital, technology or telecom services, including use of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software

☐ Journalism and media, including the processing of journalistic, literary or artistic material made or intended to be made available to the public or any section of the public.

☐ Legal services, including advising and acting on behalf of clients.

☐ Licensing and registration, including the administration of licensing or maintenance of official registers.

☐ Not-for-profit organisations' activities, including

• establishing or maintaining membership of or support for a not-for-profit body or association, and
• providing or administering activities for individuals who are either members of the not-for-profit body or association or have regular contact with it.

☐ Pastoral care, including the administration of pastoral care by a vicar or other minister of religion.

☐ Pensions administration, including the administration of funded pensions or superannuation schemes.

☐ Procurement, including deciding whether to accept any person or organisation as a supplier, and the administration of contracts, performance measures and other records.

☐ Private investigation, including the provision on a commercial basis of investigatory services according to instruction given by clients

☐ Property management, including the management and administration of land, property and residential property, and the estate management of other organisations.

☐ Realising the objectives of a charitable organisation or voluntary body, including the provision of goods and services in order to realise the objectives of the charity or voluntary body.

☐ Research in any field, including market, health, lifestyle, scientific or technical research.

☐ Security of people and property, including using CCTV systems for this purpose.

☐ Trading/sharing in personal information, including the sale, hire, exchange or disclosure of personal information to third parties in return for goods/services/benefits.

| | |
|---|---|
| ☐ Other activities (please provide details): | |
| **Data importer** | |
| The data importer is (please specify briefly your activities relevant to the transfer):<br><br>*Please select one option:*<br>☐ Option 1: The data importer is (please specify briefly your activities relevant to the transfer):<br><br>☑ Option 2: The following checklist and other details set out, in brief, what the data importer is and its activities relevant to the transfer:<br><br><br>**The data importer's business or organisation type is:**<br><br>☐ Central government<br><br>☐ Charitable and voluntary<br><br>☐ Education and childcare<br><br>☐ Finance, insurance and credit<br><br>☐ General business<br><br>☐ Health<br><br>☑ IT, digital, technology and telecoms<br><br>☐ Justice and policing<br><br>☐ Land and property services<br><br>☐ Legal and professional advisers<br><br>☐ Local government<br><br>☐ Marketing and research<br><br>☐ Media<br><br>☐ Membership association<br><br>☐ Political<br><br>☐ Regulators<br><br>☐ Religious<br><br>☐ Research<br><br>☐ Retail and manufacture<br><br>☐ Social care | → **ACTION**: Set out the importer's type of business and its activities relevant to the restricted transfer.<br><br>You have two options:<br><br>Option 1. You may set this out in your own words. As a suggestion, you could use the following form:<br><br>**The data importer is:** insert description of importer. **The data importer's activities which are relevant to the restricted transfer are:** add activities.<br><br>For example:<br>"The data importer is a US-based supplier of software solutions. It is supplying a software package to the exporter and will host the importer's customer data on its servers in the US."<br><br>You should also have a controller-processor contract in place. If so, you may be able to re-use a description of the importer's activities as set out in that contract.<br><br>Option 2: you may find it easier to use the checklists provided.<br><br>Instructions:<br>Step 1: Think about the importer's type of business or organisation and click in the box next to the appropriate category, making appropriate amendments or adding specific detail.<br><br>Step 2: Think about why the data importer is using the personal data to be transferred. Click in the box next to all of the activities which apply, making appropriate amendments or adding specific details. You can click "other" and add your own description at the end. |

☐ Trade, employer associations, and professional bodies

☐ Traders in personal data

☐ Transport and leisure

☐ Utilities and natural resources

☐ Other – Please add details:          activities

**The data importer's activities for the data exporter, which are relevant to the transfer are:**

☐ Accounts and records services, including

☐ Accounts and records services, including
• Keeping accounts;
• Keeping records of purchases, sales or other transactions, including payments, deliveries or services provided by the data exporter or to the data exporter;
• Records for making financial or management forecasts
• Other general records and information forecasts

- Other general records and information management services.

☐ Administration services relating to membership or supporter records.

☐ Advertising, marketing, and public relations services.

☐ Auditing services

☐ Facilities management services, including cleaning, catering, reception, security, maintenance, gardening, events management, business travel, meetings, vehicle hire, copying, printing and post services.

☐ Benefits, grants and loans administration services.

☐ Consultancy and general advisory services.

☐ Debt administration and factoring services, including the tracing of consumer and commercial debtors and the collection on behalf of creditors.

☐ Education or training services.

☐ Financial services administration and advice services including the provision of services as an intermediary in respect of any financial transactions including mortgage and insurance broking.

☐ Fundraising services.

☐ Health administration and health services, including the provision and administration of patient care.

☐ Information and databank administration, including the maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.

☐ Insurance administration including the administration of life, health, pensions, property, motor and other insurance business.

☑ IT, digital, technology or telecom services, including provision of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software licensing

☐ Legal administration and legal support services.

☐ Licensing and registration services, including the administration of licensing or maintenance of official registers.

☐ Media services.

| | |
|---|---|
| ☐ Pensions administration, including the administration of funded pensions or superannuation schemes. | |
| ☐ Property management services, including the management and administration of land, property and residential property, and the estate management of other organisations. | |
| ☐ Procurement services, including deciding whether to accept any person or organisation as a supplier, and the administration of contracts, performance measures and other records. | |
| ☐ Provision of temporary and agency staff. | |
| ☐ Research and development services, including market, health, lifestyle, scientific or technical research. | |
| ☐ Services in relation to the assessment and collection of taxes, duties, levies and other revenue. | |
| ☐ Services in relation to trading/sharing in personal information, including the sale, hire, exchange or disclosure of personal information to third parties in return for goods/services/benefits. | |
| ☐ Staff administration services, including appointment or removals, pay, discipline; superannuation, training, employee benefits, work management, and other personnel matters in relation to the data exporter's staff. | |
| ☐ Other services (please provide a description): | |
| **Data subjects** | |
| The personal data transferred concern the following categories of data subjects (please specify): | → **ACTION**: The parties should list the categories of data subject. |
| Each category includes current, past and prospective data subjects. Where any of the following is itself a business or organisation, it includes their staff. | Instructions: Think about who the personal data being transferred is about, and click in the box next to all of the categories of data subjects which are included in the personal data being transferred. |
| ☐ staff including volunteers, agents, temporary and casual workers | You may make appropriate amendments or add specific details to any of the categories or click "other" and add your own categories at the end. |

☑ customers and clients (including their staff)

☐ suppliers (including their staff)

☐ members or supporters

☐ shareholders

☐ relatives, guardians and associates of the data subject

☐ complainants, correspondents and enquirers;

☐ experts and witnesses

☐ advisers, consultants and other professional experts

☐ patients

☐ students and pupils

☐ offenders and suspected offenders

☐ other (please provide details of other categories of data subjects):

| Categories of data | |
| --- | --- |
| The personal data transferred concern the following categories of data (please specify): | → **ACTION**: The parties should list the categories of personal data being transferred. |
| The following is a list of standard descriptions of categories of data: | Instructions: Think about what the personal data being transferred is about and click in the box next to all of the categories of personal data which are being transferred |
| ☑ Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description. | You may make appropriate amendments or add specific details to any of the categories, or click "other" and add your own categories at the end. |
| ☐ Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, driving licence details. | |
| ☐ Family, lifestyle and social circumstances, including any information relating to the family of the data subject and the data subject's lifestyle and social circumstances, including current marriage and partnerships, marital history, details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organisations. | |
| ☐ Education and training details, including information which relates to the education and any professional training of the data subject, including academic | |

| | |
|---|---|
| records, qualifications, skills, training records, professional expertise, student and pupil records.<br><br>☐ Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records, and security records.<br><br>☐ Financial details, including information relating to the financial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, and pension information.<br><br>☑ Goods or services provided and related information, including details of the goods or services supplied, licences issued, and contracts.<br><br>☐ Personal data relating to criminal convictions and offences<br><br>☐ Other (please provide details of other data subjects): | |
| **Special categories of data (if appropriate)** | |
| The personal data transferred concern the following special categories of data (please specify):<br><br>Personal data which is on, which reveals, or which concerns:<br>☐ racial or ethnic origin<br>☐ political opinions<br>☐ religious or philosophical beliefs<br>☐ trade union membership<br>☐ genetic data<br>☐ biometric data (if used to identify a natural person)<br>☐ health<br>☐ sex life or sexual orientation<br>☐ criminal convictions and offences<br>☑ none of the above | → **ACTION**:<br>Include a list of any of the special categories of data which are being transferred:<br><br>For completeness, and to ensure the Clauses work under the UK GDPR, we have included the new special categories of data added by the UK GDPR and criminal convictions and offences data.<br><br>Instructions: Think about the set of personal data being transferred and click in the box next to any of the special categories of data or criminal records and convictions data, which are included. |
| **Processing operations** | |
| The personal data transferred will be subject to the following basic processing activities (please specify): | → **ACTION**: List the processing activities which may be carried out.<br><br>Instructions: Think about how the data importer will be using and handling the set of personal data transferred to it, and click in the box next to all of the processing activities which apply. |

| | |
|---|---|
| ☑ Receiving data, including collection, accessing, retrieval, recording, and data entry | You may make appropriate amendments or add specific details to any of the categories, or click "other" and add your own categories at the end. |
| ☑ Holding data, including storage, organisation and structuring | |
| ☐ Using data, including analysing, consultation, testing, automated decision making and profiling | |
| ☐ Updating data, including correcting, adaptation, alteration, alignment and combination | |
| ☑ Protecting data, including restricting, encrypting, and security testing | |
| ☑ Sharing data, including disclosure, dissemination, allowing access or otherwise making available | |
| ☐ Returning data to the data exporter or data subject | |
| ☐ Erasing data, including destruction and deletion | |
| ☐ Other (please provide details of other types of processing): | |

| | |
|---|---|
| **EXPORTER**<br><br>Authorised Signature … | → **ACTION**: The exporter should fill in this section with the:<br>• Full name of the person signing. This must be the same person throughout the document.<br>• Their position.<br>• Their business addresses.<br>**And sign where indicated**. |

| | |
|---|---|
| **DATA IMPORTER**<br>Name:<br>Stuart Henrickson<br>Secretary, Treasurer<br>Authorised Signature …   DocuSigned by:<br>*Stuart Henrickson*<br>D0E4C40BFCDD429… | → **ACTION**: The importer should fill in this section with the:<br>• Full name of the person signing. This must be the same person throughout the document.<br>• Their position.<br>• Their business addresses.<br>**And sign where indicated**. |

| Appendix 2 | **Non-legally binding guidance** |
|---|---|
| This Appendix forms part of the Clauses and must be completed and signed by the parties.<br><br>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):<br><br>*Please click in a box to select one option:*<br>☑ Option 1: Please refer to the description of the importer's security measures set out | → **ACTION**: The parties should fill in Appendix 2 with details of the security measures which the importer will provide for the transferred data.<br><br>You should also have a controller-processor contract in place, this is often the main service contract you have between you. If so, you may refer to or re-use the importer's security measures set out in that contract.<br><br>There are 3 main options for completing this Appendix.<br><br>Option 1: simply add in the name and date of the main service contract, to refer to the description of the importer's security measures contained in that agreement. |

in the contract between the controller and processor, named ⬚ Data Processing Addendum ⬚ dated

☐ Option 2: The following is the description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

☐ Option 3: The following checklist and supplementary details set out the description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5 (c):

☐ **We use firewalls to protect our internet connection** This will be your first line of defence against an intrusion from the internet.

Supplementary details of firewalls used (add any relevant details):

☐ **We choose the most appropriate secure settings for our devices and software** Most hardware and software will need some level of set-up and configuration in order to provide effective protection.

Supplementary details of security settings used (add any relevant details):

☐ **We control who has access to your data and services** Restrict access to your system to users and sources you trust.

Supplementary details of how access to your system is controlled (add any relevant details):

☐ **We protect ourselves from viruses and other malware?** Anti-virus products can regularly scan your network to prevent or detect threats.

Supplementary details of antivirus and malware protection used (add any relevant details):

☐ **We keep our software and devices up-to-date** Hardware and software needs regular updates to fix bugs and security vulnerabilities.

Supplementary details of how software and devices are kept up to date (add any relevant details, including details of the software packages, cloud services and

Option 2: insert your description of the importer's security measures there. You may choose to copy all or part of this from the main service contract.

Option 3: complete the checklist, adding in additional details which are relevant.
Instructions:
The checklist includes the baseline security measures that any business (small or large) should implement to protect its data/systems.

It is unlikely to be appropriate if the data importer is providing IT, digital, technology or telecom processor services.

This checklist for use where the transfer to the data importer and its processing of the personal data does not cause a particularly high risk to the rights of individuals. For example, where the personal data transferred is:
• not special category data;
• not criminal convictions and offences data;
• not personal details issued as an identifier by a public authority;
• not bank account, credit card or other payment data; and
• not a large volume of data.

Consider each statement, and the relevant guidance set out below, and click in the box next to those statements which apply.

Add supplementary notes to provide any further relevant detail of those security measures.

Further guidance:
• A Practical Guide to IT Security
• Cyber Security: Small Business Guide
• Cyber Essentials Scheme

| | |
|---|---|
| devices you use in processing the personal data transferred, and how you keep those updated):<br><br>☐ **We regularly backup our data** Regular backups of your most important data will ensure it can be quickly restored in the event of disaster or ransomware infection.<br><br>Supplementary details of how data is backed up (add any relevant details): | |

| | |
|---|---|
| **DATA EXPORTER**<br><br>Authorised Signature … | → **ACTION**: The exporter should fill in this section with the:<br>• Full name of the person signing. This must be the same person throughout the document. **And sign where indicated**. |
| | |

| | |
|---|---|
| **DATA IMPORTER**<br><br>Authorised Signature   ┌DocuSigned by:<br>                    *Stuart Henrickson*<br>               └D0E4C40BFCDD429…<br><br>Stuart Henrickson<br>Secretary, Treasurer | → **ACTION**: The importer should fill in this section with the:<br>• Full name of the person signing. This must be the same person throughout the document. **And sign where indicated** |

1