DATA PRIVACY & DATA SECURITY ADDENDUM
Exhibit to Axcient Partner Agreement

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

1. Definitions

"**Authorized Persons**" means Axcient's employees, agents, and contractors that have a need to know or otherwise access Customer Data to enable Axcient to perform the Services.
"Adequate Country" means a country or territory that the recognised under applicable Data Protection Laws from time to time as providing adequate protection for personal data.
"**Controller**" means a controller as defined under the General Data Protection Regulation (GDPR).
"**Customer Data**" means all data relating to Customer that is (i) provided to Axcient by or on behalf of Customer or (ii) otherwise obtained, accessed, developed, or produced by Axcient. Customer Data includes Personal Data.
"**Data Protection Laws**" means all international, federal, national and state privacy and data protection laws and regulations to the extent applicable to Axcient and the Services, including, without limitation, the General Data Protection Regulation 2016/679 (the "**GDPR**"), UK Data Protection Law and all national and other legislation implementing or supplementing the foregoing, all as amended, re-enacted and/or replaced and in force from time to time.
"**Data Breach**" means any loss or unauthorized access, acquisition, theft, destruction, disclosure or use of Customer Data that occurs while such Customer Data is in the possession of or under the control of Axcient.
"**Parties**" means Customer and Axcient.
"**Personal Data**" means information relating to an identified or identifiable natural person (the "**Data Subject**") Processed by Axcient pursuant to the MSA. An identifiable natural person is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
"**Process**" or "**Processing**" means any operation or set of operations that are performed upon Customer Data, whether or not by automatic means, such as collection, accessing, processing, use, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, transmittal, alignment or combination, blocking, erasure, destruction or otherwise used as set out in the applicable Data Protection Laws.
"**Processor**" means a processor as defined under the GDPR.
"**Services**" means the services, products and other activities to be provided to or carried out by or on behalf of Axcient for Customer pursuant to the MSA.
"**Standard Contractual Clauses**" means the model clauses for the transfer of personal data to processors established in third countries approved by the European Commission, the approved version of which is set out in the European Commission's Decision 2010/87/EU of 5 February 2010 and at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 and which along with the Appendices to the Standard Contractual Clauses included in Annex 1 to this Addendum, form a part of this Addendum.
"**Sub-Processor**" shall mean an entity engaged by Axcient to assist it in Processing the Customer Data in fulfilment of its obligations under the MSA.
"**Third Party**" is any person or entity other than Axcient and Customer.
"**UK Data Protection Law**" means the Data Protection Act 2018 of the United Kingdom and the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 as amended, re-enacted and/or replaced and in force from time to time.

2. Data Privacy.

2.1 Compliance with Laws. The Parties shall comply with their obligations under all Data Protection Laws. For purposes of the GDPR, Customer is considered the Controller and Axcient is its Processor for the Processing of Personal Data in connection with the Services provided under the MSA. If Customer is considered a Processor for purposes of the GDPR, then Axcient is considered its Sub-Processor.
2.2 The type of Personal Data Processed pursuant to this Addendum and the subject matter, duration, nature and purpose of the Processing, and the categories of Data Subjects, are as described below:

(a) Subject matter of the Processing: Axcient's provision of the Services to the Customer.

(b) nature and purpose of the Processing: the collection, analysis, storage, duplication, deletion and disclosure as necessary to provide the Services and as may be further instructed by Customer in writing.

(c) Duration of Processing: Axcient will process the Personal Data for the duration of the MSA, or until the Processing of the Personal Data is no longer necessary for the purposes of either party performing its obligations under the MSA (to the extent applicable) unless otherwise agreed between the parties in writing.

(d) Types of data: data relating to individuals provided to Axcient via the Services, by (or at the direction of) Customer.

(e) Categories of data subjects: data subjects may include Customer's customers, employees, suppliers and end users about whom data is provided to Axcient via the Services by (or at the direction of) the Customer.

2.3 Distribution of Customer Data. Customer shall only provide Axcient with Personal Data that is needed by Axcient to provide the Services to Customer. Axcient shall not be responsible for any additional Personal Data. Customer represents and warrants that it has complied with applicable law in collecting the Personal Data including obtaining any necessary consents from any Controller or Data Subject to provide the Personal Data that it makes available to Axcient pursuant to this Addendum.

2.4 Limitations on Use of Personal Data. Axcient shall not Process Customer Data other than in accordance with the Customer's instructions and this Addendum. If any of the Customer's instructions, in Axcient's opinion, infringe Data Protection Laws, Axcient shall inform the Customer as soon as reasonably practicable.

.

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

2.6 Axcient shall take reasonable steps to ensure that only authorised personnel have access to such Personal Data and that any persons whom it authorises to have access to the Personal Data are under obligations of confidentiality.

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

3. Sub-Processors.

3.1 Customer grants Axcient a general authorisation to engage Sub-Processors in connection with the provision of the Services.. Upon Customer's request, Axcient shall provide Customer with a list of Sub-Processors and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data. If Company has a reasonable objection to any Sub-Processor, it shall notify Axcient of such objections in writing within ten (10) days of the receiving the list of Sub-Processors and the parties will seek to resolve the matter in good faith. If Axcient is reasonably able to provide the Services to Customer in accordance with the MSA without using the Sub-Processor and decides to do so, then Customer will have no further rights under this clause 3.1 in respect of the proposed use of the Sub-Processor. If Axcient requires use of the Sub-Processor in its discretion and is unable to satisfy Customer as to the suitability of the Sub-Processor or the documentation and protections in place between Customer and the Sub-Processor within ninety (90) days from Customer's notification of objections, Customer may within thirty (30) days following the end of the ninety (90) day period referred to above, terminate the MSA or the applicable services (as Customer may decide) with at least thirty (30) days' written notice. If Customer does not provide a timely objection to any new or replacement Sub-Processor in accordance with this clause 3.1 Customer will be deemed to have consented to the Sub-Processor and waived its right to object. Axcient may use a new or replacement Sub-Processor whilst the objection procedure in this clause 3.1 is in process.

3.2 Axcient shall ensure that any sub-processor it engages to provide an aspect of the Services on its behalf in connection with this Addendum does so only on the basis of a written contract which imposes on such sub-processor terms substantially equivalent to those imposed on Axcient in this Addendum (the "**Relevant Terms**"). Axcient shall procure the performance by such sub-processor of the Relevant Terms and shall be liable to Customer for any breach by such person of any of the Relevant Terms.

4. Cooperation.

4.1 Axcient shall use commercially reasonable efforts to cooperate and assist the Customer with a Data Subject's exercise of his/her rights under applicable Data Protection Laws with respect to Personal Data Processed by Axcient, including, without limitation, the right to be forgotten, the right to data portability, and the right to access data under the GDPR. Axcient shall promptly notify Customer if Axcient receives any such request.
4.2 Axcient shall provide commercially reasonable efforts to provide such assistance to Customer as Customer requests in relation to Customer's obligations under the Data Protection Laws with respect to: (i) data protection impact assessments (as such term is defined in the GDPR and/or UK Data Protection Law where applicable); (ii) notifications to the supervisory authority under EU Data Protection Laws and/or communications to data subjects by Customer in response to any Security Breach; and (iii) Customer's compliance with their respective obligations under the GDPR and/or UK Data Protection Law where applicable with respect to the security of Processing.

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

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

7. Data Breach Procedures.
7.1 Notification. Axcient shall notify Customer of any Data Breach as soon as practicable and without undue delay after becoming aware of it. Such notification shall at a minimum: (i) describe the nature of the Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned; (ii) communicate the name and contact details of Axcient's data protection officer or other relevant contact from whom more information may be obtained; and (iii) describe the measures taken or proposed to be taken to address the Data Breach.
7.2 Remedial Actions. In the event of a Data Breach caused by Axcient, Axcient will use commercially reasonable efforts to: (a) remedy the Data Breach condition, investigate, document, restore Customer service(s), and undertake required response activities; (b) provide regular status reports to Customer on Data Breach response activities; (c) assist Customer with the coordination of media, law
enforcement, or other Data Breach notifications; and (d) assist and cooperate with Customer in its Data Breach response efforts.

8. Cross-Border Transfers.
8.1 Location. The Customer acknowledges that Axcient systems and Axcient's Processing of Customer Data will occur within the United States of America (the "**Processing Jurisdiction**"), and the parties agree that the Standard Contractual Clauses shall apply to any transfer of Personal Data from the Customer in the European Economic Area ("**EEA**") to Axcient.
8.2 Sub-Processors. If in the performance of this Addendum, Axcient transfers any Personal Data to a Sub-Processor located, or permits Processing of any Personal Data by a Sub-Processor outside of the EEA except

if in or to an Adequate Country, Axcient shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that Processing, such as the requirement that Axcient to execute or procure that the Sub-Processor execute Standard Contractual Clauses.
8.3 Customer may exercise its rights under the Standard Contractual Clauses in respect of the appointment of Sub-Processors and audit as set out in sections 3.1 and 10 respectively of this Addendum.

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

10. Audits Reports.
10.1Without limiting any of Axcient's other obligations under this Article 10, if Axcient engages a third party auditor to perform a SOC 2 or other data security audit of Axcient's operations, information security program or disaster recovery/business continuity plan, Axcient, at Customer's written request, shall provide a copy of the audit report to Customer. Any such audit reports shall be Axcient's confidential information.
10.2 Axcient shall, in accordance with the Data Protection Laws make available to Customer such information in Axcient's possession or control, and provide all assistance in connection with audits of Axcient's premises, systems and documentation as Customer may reasonably request with a view to demonstrating Axcient's compliance with the obligations of Processors under the Data Protection Laws in relation to its Processing of Personal Data.

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

12. Miscellaneous.
12.1 Conflicts. In the event of any conflict or inconsistency between the provisions of this Addendum and the provisions of the MSA, the provisions of this Addendum shall prevail.
12.2 Governing Law. This Addendum shall be governed by and construed in accordance with the choice of law in the MSA.

ANNEX 1 STANDARD CONTRACTUAL CLAUSES
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

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

Name of the data exporting organisation:

Address:

Tel.

Fax

e-mail: …

Other information needed to identify the organisation:

(the data **exporter**)

And

Name of the data importing organisation:

Address:

Tel.

Fax:

e-mail:

Other information needed to identify the organisation:

(the data **importer**)

each a ‘party’; together ‘the parties’,

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

Clause 1

Definitions

For the purposes of the Clauses:

(a)‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ([1]);

(b) ‘the data exporter’ means the controller who transfers the personal data;

(c)‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(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;

(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 Member State in which the data exporter is established;

(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 access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer [2]

The data importer agrees and warrants:

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

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

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

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

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

(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;

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

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

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

Clause 9

Governing law

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

Clause 10

Variation of the contract

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

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses ([3]). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely …
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

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

	Signature

On behalf of the data importer:

Name (written out in full):

Position:

Address:

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

	Signature

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Appendix 1

to the Standard Contractual Clauses

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

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

Data exporter

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

…

…

…

Data importer

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

…

…

…

Data subjects

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

…

…

…

Categories of data

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

…

…

…

Special categories of data (if appropriate)

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

…

…

…

Processing operations

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

…

…

…

DATA EXPORTER

Name:

Authorised Signature

DATA IMPORTER

Name:

Authorised Signature

Appendix 2

to the Standard Contractual Clauses

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

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

…

…

…

…

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

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 first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b)the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim ([1]).

[1] Paragraph on liabilities is optional.