SUPPLIER DATA PROCESSING ADDENDUM [v1.1 20180605]

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

Definitions

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

“Addendum Effective Date” means the effective date of the Principal Agreement.

"Authorised Sub-processors" means (a) those Sub-processors set out in Annex 3 (Authorised Transfers of Controller Personal Data); and (b) any additional Sub-processors consented to in writing by Controller in accordance with Sub-processing section.

“***Controller***” is the party defined as such in the Principal Agreement.

"Controller Personal Data" means the data described in Annex 1 and any other Personal Data processed by the Processor on behalf of the Controller pursuant to or in connection with the Principal Agreement**.**

“Data Protection Laws” means EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR") as well as any local data protection laws***.***

"EEA" means the European Economic Area.

“Erasure" means the removal or destruction of Personal Data such that it cannot be recovered or reconstructed***.***

"Personal Data Breach" means a breach of leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Controller Personal Data transmitted, stored or otherwise processed***.***

“Principal Agreement” means the agreement between the Controller and the Processor incorporating this Addendum.

“***Processor***” is the party defined as such in the Principal Agreement.

"Process/Processing/Processed", "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Special Categories of Personal Data" and any further definition not included under this Addendum or the Principal Agreement have the same meaning as in EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR").

“Products” means the products supplied by, or to be supplied, by the Processor to the Controller pursuant to the Principal Agreement***.***

"Sub-processor" means any Data Processor (including any third party) appointed by the Processor to process Controller Personal Data on behalf of the Controller.

"Services" means the services supplied, or to be supplied, by the Processor to the Controller pursuant to the Principal Agreement***.***

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to Processors established in third countries, as approved by the European Commission Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these.

***"Third Country*"** means any country outside EU/EEA, except where that country is the subject of a valid adequacy decision by the European Commission on the protection of Personal Data in Third Countries.

Data Processing Terms

1. In the course of providing the Services and/or Products to the Controller pursuant to the Principal Agreement, the Processor shall process Controller personal data on behalf of the Controller in accordance terms of this Addendum. The Processor shall comply with the following provisions with respect to any Controller personal data.
2. To the extent required by applicable Data Protection Laws, the Processor shall obtain and maintains all necessary licenses, authorisations and permits necessary to process personal data including personal data mentioned in Annex 1.

The Processor shall maintain all the technical and organisational measures to comply with the requirements set forth in this Addendum and its Annexes.

Processing of Controller Personal Data

1. The Processor shall only process Controller Personal Data for the purposes of the Principal Agreement. The Processor shall not process, transfer, modify, amend or alter the Controller Personal Data or disclose or permit the disclosure of the Controller Personal Data to any third party other than in accordance with Controller's written instructions, unless processing is required by EU or Member State law to which the Processor is subject. The Processor shall, to the extent permitted by such law, inform the Controller of that legal requirement before processing the Personal Data and comply with the Controller's instructions to minimise, as much as possible, the scope of the disclosure.

2. For the purposes set out in section above, the Controller hereby instructs the Processor to transfer Controller Personal Data to the recipients in the Third Countries listed in Annex 3 (Authorised Transfers of Controller Personal Data), always provided that Processor shall comply with section Sub-processing.

Reliability and Non–Disclosure

1. The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Controller personal data, ensuring in each case that access is strictly limited to those individuals who require access to the relevant Controller Personal Data.

2. The Processor must ensure that all individuals which have a duty to process controller personal data:
    a. Are informed of the confidential nature of the Controller Personal Data and are aware of Processor's obligations under this Addendum and the Principal Agreement in relation to the Controller Personal Data;
    b. Have undertaken appropriate training/certifications in relation to the Data Protection Laws or any other training/certifications requested by Controller;
    c. Are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and
    d. Are subject to user authentication and logon processes when accessing the Controller Personal Data in accordance with this Addendum, the Principal Agreement and the applicable Data Protection Laws.

Personal Data Security

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 risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures (Annex 2) to ensure a level of Controller Personal Data security appropriate to the risk, including but not limited to:
    a. Pseudonymisation and encryption;

   b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   c. The ability to restore the availability and access to Controller Personal Data in a timely manner in the event of a physical or technical incident; and
   d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.
   e. In assessing the appropriate level of security, the Processor shall take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Controller Personal Data transmitted, stored or otherwise processed.

Sub-Processing

1. As of the Addendum Effective Date, the Controller hereby authorises the Processor to engage those Sub-processors set out in Annex 3 (Authorised Transfers of Controller Personal Data). The Processor shall not engage any Data Sub-Processors to Process Controller Personal Data other than with the prior written consent of Controller, which Controller may refuse with absolute discretion.
2. With respect to each Sub-processor, the Processor shall:
   a. Provide the Controller with full details of the Processing to be undertaken by each Sub-processor.
   b. Carry out adequate due diligence on each Sub-processor to ensure that it can provide the level of protection for Controller Personal Data, including without limitation, sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of GDPR, this Addendum, the Principal Agreement and the applicable Data Protection Laws.
   c. Include terms in the contract between the Processor and each Sub-processor which are the same as those set out in this Addendum. Upon request, the Processor shall provide a copy of its agreements with Sub-processors to Controller for its review.
3. Insofar as that contract involves the transfer of Controller Personal Data outside of the EEA, incorporate the Standard Contractual Clauses or such other mechanism as directed by the Controller into the contract between the Processor and each Sub-processor to ensure the adequate protection of the transferred Controller Personal Data. In such situations, evidence of such undertakings shall be provided. This can include, but not limited to, certificates of assurances and/or details of the additional measures undertaken.
4. Remain fully liable to the Controller for any failure by each Sub-processor to fulfil its obligations in relation to the Processing of any Controller Personal Data.
5. As of the Addendum Effective Date, the Controller hereby authorises the Processor to engage those Sub-processors set out in Annex 3 (Authorised Transfers of Controller Personal Data).

Data Subject Rights

1. Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising Data Subject rights as laid down in EU GDPR.
2. The Processor shall promptly notify the Controller if it receives a request from a Data Subject, the Supervisory Authority and/or other competent authority under any applicable Data Protection Laws with respect to Controller Personal Data.
3. The Processor shall cooperate as requested by the Controller to enable the Controller to comply with any exercise of rights by a Data Subject under any Data Protection Laws with respect to Controller Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws with respect to Controller Personal Data or this Addendum, which shall include:
   a. The provision of all data requested by the Controller within any reasonable timescale specified by the Controller in each case, including full details and copies of the complaint, communication or request and any Controller Personal Data it holds in relation to a Data Subject.

   b. Where applicable, providing such assistance as is reasonably requested by the Controller to enable the Controller to comply with the relevant request within the timescales prescribed by the Data Protection Laws.
   c. Implementing any additional technical and organisational measures as may be reasonably required by the Controller to allow the Controller to respond effectively to relevant complaints, communications or requests.

Personal Data Breach

1. The Processor shall notify the Controller without undue delay and, in any case, within twenty-four (24) hours upon becoming aware of or reasonably suspecting a Personal Data Breach. The Processor will provide the Controller with sufficient information to allow the Controller to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Such notification shall as a minimum:
   a. Describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
   b. Communicate the name and contact details of the Processor's Data Protection Officer, Privacy Officer or other relevant contact from whom more information may be obtained;
   c. Describe the estimated risk and the likely consequences of the Personal Data Breach; and
   d. Describe the measures taken or proposed to be taken to address the Personal Data Breach.
2. The Processor shall co-operate with the Controller and take such reasonable steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach.
3. In the event of a Personal Data Breach, the Processor shall not inform any third party without first obtaining the Controller's prior written consent, unless notification is required by EU or Member State law to which the Processor is subject, in which case the Processor shall, to the extent permitted by such law, inform the Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Controller before notifying the Personal Data Breach.

Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments which are required under Article 35 of GDPR and with any prior consultations to any supervisory authority of the Controller which are required under Article 36 of GDPR, in each case solely in relation to Processing of Controller Personal Data by the Processor on behalf of the Controller and considering the nature of the processing and information available to the Processor.

Erasure or return of Controller Personal Data

1. Processor shall promptly and, in any event, within 90 (ninety) calendar days of the earlier of: (i) cessation of Processing of Controller Personal Data by Processor; or (ii) termination of the Principal Agreement, at the choice of Controller (such choice to be notified to Processor in writing) either:
   a. Return a complete copy of all Controller Personal Data to the Controller by secure file transfer in such format as notified by the Controller to the Processor and securely erase all other copies of Controller Personal Data Processed by the Processor or any Authorised Sub-processor; or
   b. Securely wipe all copies of Controller Personal Data Processed by Processor or any Authorised Sub-processor, and in each case, provide a written certification to the Controller that it has complied fully with the requirements of section Erasure or Return of Controller Personal Data.
2. Processor may retain Controller Personal Data to the extent required by Union or Member State law, and only to the extent and for such period as required by Union or Member State law, and always provided that Processor shall ensure the confidentiality of all such Controller

Personal Data and shall ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Union or Member State law requiring its storage and for no other purpose.

Audit rights

1. Processor shall make available to the Controller, upon request, all information necessary to demonstrate compliance with this Addendum and allow for, and contribute to audits, including inspections by the Controller or another auditor mandated by the Controller of any premises where the Processing of Controller Personal Data takes place.

2. The Processor shall permit the Controller or another auditor mandated by the Controller to inspect, audit and copy any relevant records, processes and systems in order that the Controller may satisfy itself that the provisions of this Addendum are being complied with.

3. The Processor shall provide full cooperation to the Controller with respect to any such audit and shall, at the request of the Controller, provide the Controller with evidence of compliance with its obligations under this Addendum. Processor shall immediately inform the Controller if, in its opinion, an instruction pursuant to this section Audit (Audit Rights) infringes the GDPR or other EU or Member State data protection provisions.

International Transfers of Controller Personal Data

Processor shall not process Controller Personal Data nor permit any Authorised Sub-processor to process the Controller Personal Data in a Third Country, other than with respect to those recipients in Third Countries (if any) listed in Annex 3 (Authorised Transfers of Controller Personal Data), unless authorised in writing by Controller in advance, via an amendment to this Addendum.

When requested by Controller, Processor shall promptly enter into (or procure that any relevant Sub-processor of Processor enters into) an agreement with Controller including Standard Contractual Clauses and/or such variation as Data Protection Laws might require, in respect of any processing of Controller Personal Data in a Third Country, which terms shall take precedence over those in this Addendum.

Codes of Conduct and Certification

At the request of the Controller, the Processor shall comply with any Code of Conduct approved pursuant to Article 40 of GDPR and obtain any certification approved by Article 42 of EU GDPR, to the extent that they relate to the processing of Controller Personal Data.

General Terms

1. Any obligation imposed on the Processor under this Addendum in relation to the Processing of Personal Data shall survive any termination or expiration of the Principal Contract.

2. Any breach of this Addendum shall constitute a material breach of the Principal Agreement.

3. With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including but not limited to the Principal Agreement, the provisions of this Addendum shall prevail with regard to the parties’ data protection obligations for Personal Data of a Data Subject from a Member State of the European Union.

4. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

5. In accordance with Article 26(2) of Directive 95/46/EC the Processor shall enter into an agreement in the form at Annex 4 below prior to transfer of any Personal Data to processors established in a Third Country. A copy of the executed agreement shall be provided to the Controller by the Processor prior to transfer of Personal Data to a Third Country.

ANNEX 1: DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

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

Subject matter and duration of the Processing of Controller Personal Data

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

The nature and purpose of the Processing of Controller Personal Data

[Include description here]

The types of Controller Personal Data to be Processed

[Include list of data types here]

The categories of Data Subject to whom the Controller Personal Data relates

[Include categories of data subjects here]

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

Security Management

a) Security policy and procedures: Processor must document a security policy with regard to the processing of personal data.

b) Roles and responsibilities :

   a) Roles and responsibilities related to the processing of personal data is clearly defined and allocated in accordance with the security policy.

   b) During internal re-organisations or terminations and change of employment, revocation of rights and responsibilities with respective hand-over procedures is clearly defined.

c) Access Control Policy: Specific access control rights are allocated to each role involved in the processing of personal data, following the need-to-know principle.

d) Resource/asset management: Processor has a register of the IT resources used for the processing of personal data (hardware, software, and network). A specific person is assigned the task of maintaining and updating the register (e.g. IT officer).

e) Change management: Processor makes sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process takes place.

Incident response and business continuity

a) Incidents handling / Personal data breaches:

   a. An incident response plan with detailed procedures is defined to ensure effective and orderly response to incidents pertaining personal data.

   b. Processor will report without undue delay to Controller any security incident that has resulted in a loss, misuse or unauthorised acquisition of any personal data.

b) Business continuity: Processor establishes the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).

Human resources

a) Confidentiality of personnel: Processor ensures that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.

b) Training: Processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

Technical security measures

1. Access control and authentication

a) An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing and deleting user accounts.

b) The use of common user accounts is avoided. In cases where this is necessary, it is ensured that all users of the common account have the same roles and responsibilities.

c) When granting access or assigning user roles, the “need-to-know principle” shall be observed in order to limit the number of users having access to personal data only to those who require it for achieving the Processor’s processing purposes.

d) Where authentication mechanisms are based on passwords, Processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

e) The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.

Logging and monitoring

Log files are activated for each system/application used for the processing of personal data. They include all types of access to data (view, modification, deletion).

Security of data at rest

Server/Database security

a) Database and applications servers are configured to run using a separate account, with minimum OS privileges to function correctly.
b) Database and applications servers only process the personal data that are actually needed to process in order to achieve its processing purposes.

Workstation security:
a) Users are not able to deactivate or bypass security settings.
b) Anti-virus applications and detection signatures is configured on a regular basis.
c) Users don't have privileges to install or deactivate unauthorised software applications.
d) The system has session time-outs when the user has not been active for a certain time period.
e) Critical security updates released by the operating system developer is installed regularly.

Network/Communication security:
a) Whenever access is performed through the Internet, communication is encrypted through cryptographic protocols.
b) Traffic to and from the IT system is monitored and controlled through Firewalls and Intrusion Detection Systems.

Back-ups:
a) Backup and data restore procedures are defined, documented and clearly linked to roles and responsibilities.
b) Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.
c) Execution of backups is monitored to ensure completeness.

Mobile/Portable devices:
a) Mobile and portable device management procedures are defined and documented establishing clear rules for their proper use.
b) Mobile devices that are allowed to access the information system is pre-registered and pre-authorised.

Application lifecycle security:
During the development lifecycle, best practice, state of the art and well acknowledged secure development practices or standards is followed.

Data deletion/disposal:
a) Software-based overwriting will be performed on media prior to their disposal. In cases where this is not possible (CD’s, DVD’s, etc.) physical destruction will be performed.
b) Shredding of paper and portable media used to store personal data is carried out.

Physical security:
The physical perimeter of the IT system infrastructure is not accessible by non-authorised personnel. Appropriate technical measures (e.g. Intrusion detection system, chip-card operated turnstile, single-person security entry system, locking system) or organisational measures (e.g., security guard) shall be set in place to protect security areas and their access points against entry by unauthorised persons.

ANNEX 3: AUTHORISED TRANSFERS OF CONTROLLER PERSONAL DATA

List of Approved Sub-processors as at the Addendum Effective Date to be included in the Principal Contract in the form set out below including the (i) full legal name; (ii) processing activity; (iii) location of service centre(s).

No.	Authorised sub-processor (full legal name)	Processing activity	Location of service centre(s).
1.	…………….		

Annex 4

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:.. ;e-mail:.....................................

Other information needed to identify the organisation:

………………………………………………………………
(the data **exporter**)

And

Name of the data importing organisation:..

Address:..

Tel:... ;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;

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

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

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 subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and 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 subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

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 subprocessor 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 subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

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 subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

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

Subprocessing

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

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

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

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

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

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

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…………………………………….

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.