DATA PROCESSING AGREEMENT

This Addendum is incorporated into, supplements and, in the event of any conflict with respect to the protection of Personal Information, supersedes any other terms of the Master Terms Agreement with respect to matters within its scope.

1. Definitions. The following definitions shall apply in this Addendum:

   (a) "**Data Protection Law**" means all applicable law relating to privacy and the protection and processing of personal data in any relevant jurisdiction.

   (b) "**Personal Information**" means any personal data as such information is defined under applicable Data Protection Law that is accessible or provided by or on behalf of Customer to Supplier in connection with the Agreement. For example, Personal Information shall mean "nonpublic personal information" as defined under Gramm-Leach-Bliley Act of 1999 and "personal data" as defined under the EU Data Protection Directive (Directive 95/46/EC) (as may be amended, extended or re-enacted from time to time), to the extent such Data Protection Laws are applicable.

   (c) "**Personal Information Incident**" means any known or suspected accidental, unauthorized or unlawful access, acquisition, use, alteration, disclosure, loss or destruction of Personal Information.

2. Processing of Personal Information. To the extent Supplier processes Personal Information, Supplier shall:

   (a) Process Personal Information only on behalf of Customer, only for the purposes of performing the Agreement, and only in accordance with Data Protection Law and instructions contained herein or received from Customer from time to time; Personal Information processing activities hereunder are further described in the Annex 1.

   (b) not otherwise modify, amend or alter the Personal Information unless specifically authorized in writing by Customer;

   (c) ensure that only those Supplier Personnel who require access to the Personal Information for the performance of the Agreement are granted access to such Personal Information and that such Personnel are reliable, regularly trained on data protection and information security (with refresher training provided where knowledge gaps are identified or new Data Protection Laws are implemented) and informed of the confidential nature of the Personal Information and the obligations set out in the Agreement;

   (d) notify Customer in writing without undue delay, but in any event within five (5) business days, and provide full details thereof, if it receives: (i) a request from a data subject to have access to his/her Personal Information; (ii) a complaint or request made in respect of any Personal Information; or (iii) any other communication from a regulatory or government authority or data subject relating to the processing of any Personal Information;

   (e) provide Customer with reasonable cooperation and assistance in relation to any of the requests or complaints referenced in the foregoing subsection, including by complying with any timescale dictated by applicable Data Protection Law, and in all cases strictly in accordance with Customer's reasonable timescale, and providing Customer with any Personal Information it holds in relation to the data subject(s) involved and any information reasonably requested by Customer in connection therewith; and

   (f) provide Customer with all information reasonably necessary to demonstrate Supplier's compliance with this Addendum and applicable Data Protection Law.

3. Disclosure of Personal Information. To the extent Supplier processes Personal Information, Supplier shall:

   (a) obtain prior written consent from Customer before disclosing Personal Information with any third party, including Supplier's Subcontractors (such as a third party hosting Subcontractor) and Affiliates and;

   (b) prior to any disclosure, ensure that any such third party is bound by a written agreement with Customer or Supplier (as the case may be) that contains data protection provisions equivalent to those set out in the Agreement and is co-terminus with the Agreement insofar as it relates to Personal Information;

   (c) if Supplier is legally required by any subpoena, court order, or other similar process to disclose Personal Information, unless prohibited by law, (i) immediately notify Customer, (ii) provide Customer with the relevant documentation thereof, and (iii) permit Customer adequate time to exercise its legal options to prohibit or limit disclosure.

4. Export of Personal Information. To the extent Supplier processes Personal Information, Supplier shall not transfer Personal Information to any jurisdiction not expressly approved by Customer in writing, and in the event of such Customer approval, Supplier and/or its Subcontractors and Affiliates, as applicable, shall enter into any data transfer agreement that Customer reasonably considers necessary to satisfy applicable Data Protection Law and to provide an adequate level of protection to the Personal Information to be transferred.

5. European Economic Area. When Supplier processes any Personal Information as defined by the applicable Data Protection Law of the European Economic Area, the parties acknowledge and agree that, as between the parties, Customer is the *data controller* or *exporter* and Supplier is the *data processor* or *importer*. The parties agree that the italicized terms in the foregoing sentence shall have the meanings ascribed to them by applicable Data Protection Law. Transfers of such Personal Information from the Customer, located in the European Union, to the Supplier, located out of the European Union (EU), shall be governed by the Standard Contractual Clauses attached hereto as Annex 3.

6. Security of Personal Information.

   (a) Supplier will implement and maintain a comprehensive written information security program that includes all necessary measures, including the establishment and maintenance of policies and procedures as well as technical, physical, and administrative safeguards to: ensure the security and confidentiality of Personal Information; protect against any foreseeable threats or hazards to the security or integrity of Personal Information; protect against the accidental, unauthorized or unlawful access, acquisition, use, alteration, disclosure, loss or destruction of Personal Information; and ensure secure and appropriate disposal of Personal Information ("**Information Security Program**"). A summary of key aspects of the Information Security Program is attached hereto as Annex 2. At no time shall Supplier Information Security Program offer less protection of Personal Information than that described in Annex 2.

   (b) Without limiting the generality of the foregoing, the Information Security Program will provide for regular assessment (no less than annually) of the risks to the security of Personal Information processed by Supplier and its Subcontractors and Affiliates, as applicable, including: (i) identification of internal and external threats that could result in unauthorized disclosure, alteration or destruction of Personal Information and systems used by Supplier and its Subcontractors and Affiliates, as applicable, (ii) assessment of the likelihood and potential damage of such threats, taking into account the sensitivity of such Personal Information, and (iii) assessment of the sufficiency of policies, procedures, information systems of Supplier and its Subcontractors and Affiliates, as applicable, and other arrangements in place, to control risks; and appropriate protection against such risks.

(c) The Information Security Program shall also require encryption of Personal Information in electronic form while in transit or at rest, and enhanced controls and standards for transport of physical media containing Personal Information, in each case in compliance with reasonable requirements established by Customer from time to time.

(d) Supplier shall, and shall require its Subcontractors and Affiliates, as applicable, to, regularly test key controls, systems and procedures relating to the Information Security Program. The frequency and nature of such tests shall be determined by Supplier's risk assessment team, in consultation with Customer. Supplier shall provide Customer with the results of all such tests and any other audit, review or examination relating to its Information Security Program.

(e) Supplier shall periodically, and in no event less than once annually: (i) conduct risk assessments to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Supplier's Information Security Program and Supplier's processing of Personal Information, respectively; and (ii) evaluate and improve, where necessary, the effectiveness of its information security controls around the processing of Personal Information.

(f) Supplier shall provide to Customer the information set forth below, and update as necessary, for Supplier's designated individual responsible for managing, coordinating and ensuring Supplier's compliance with the obligations set forth in its Information Security Program and this Addendum.

7. Audit.

(a) Supplier shall, and shall cause Supplier's Subcontractors and Affiliates, as applicable, to assist and support Customer in any investigation by any regulator or similar authority if and to the extent that such investigation relates to Personal Information processed by Supplier and its Subcontractors and Affiliates, as applicable. Such assistance shall be at Customer's sole expense, except where such investigation was required due to failure by Supplier and/or its Subcontractors or Affiliates, as applicable, to comply with this Addendum, in which case such assistance shall be at Supplier's sole expense. Supplier and its Subcontractors and Affiliates, as applicable, shall respond to Customer's periodic and reasonable requests for information and questionnaires regarding the Information Security Program.

8. Notification of Personal Information Incidents.

(a) Supplier shall notify Customer of any Personal Information Incident without undue delay, but in any event no later than forty-eight (48) hours (unless applicable Data Protection Law or other applicable law requires notification to a regulator, government authority or data subjects of a Personal Information Incident within a shorter time period in which case Supplier shall notify Customer reasonably in advance of such notification deadline to permit Customer to reasonably prepare such notification).

(b) Supplier shall immediately investigate each Personal Information Incident, promptly provide Customer with a detailed written statement describing the circumstances surrounding each Personal Information Incident, and promptly provide and implement an appropriate remediation plan to address the Personal Information Incident and prevent any further such incidents.

9. Remedies.

(a) Notwithstanding any provision (including any limitation of liability or exclusion of consequential damages) in the Agreement, in the event of and in connection with breach by Supplier, or its Subcontractors or Affiliates, of this Addendum or applicable Data Protection Law, Supplier shall:

(i) indemnify, defend and hold harmless Customer, its Affiliates, and its and their officers, directors, employees, agents and contractors from and against all losses, liabilities, claims, damages, costs and expenses (including reasonable attorneys' fees) arising from third party claims; and

(ii) be responsible for costs incurred by Customer, its Affiliates, and its and their officers, directors, employees, agents and contractors in connection with each Personal Information Incident, including but not limited to reasonable attorneys' fees (other than in connection with third party claims), notification to any third parties or data subjects, credit monitoring for one year for data subjects, fines or penalties imposed by government or regulatory authorities, and third party crisis management services.

(b) For the sake of clarity, Customer shall decide in its sole discretion whether to notify any third parties or data subjects and the contents of any such notification(s).

10. In addition to any other rights Customer may have under this Addendum or the Agreement or at law and since unauthorized use or disclosure of Personal Information may result in immediate and irreparable injury to Customer for which monetary damages may not be adequate, in the event that Supplier, its Subcontractor and/or Affiliate, or its or their personnel uses or discloses, or, in Customer's sole opinion, is likely to use or disclose Personal Information in breach of the obligations hereunder, Customer shall be entitled to equitable relief, including temporary and permanent injunctive relief and specific performance. Customer shall also be entitled to the recovery from Supplier of any pecuniary gain realized by Supplier and/or its Subcontractors, Affiliates, or its or their personnel, as applicable, from the unauthorized use or disclosure of Personal Information.

11. Breach/Effect of Termination.

(a) Supplier shall notify Customer in writing immediately upon becoming aware of any breach by Supplier or its Subcontractors and Affiliates, as applicable, of this Addendum or applicable Data Protection Law. Such breach shall be deemed a material breach of the Agreement and in the event of such material breach, Customer may terminate any or all of the Agreement immediately upon notice to Supplier in Customer's sole discretion.

(b) Upon termination of the Agreement for any reason, Supplier shall destroy or return to Customer, per Customer's written instruction, all Personal Information (including all copies) in its possession or under its control.

ANNEX 1 - DATA PROCESSING DESCRIPTION

1. Purpose of the data Processing:

2. Categories of data subjects

3. Categories of Personal Data

The personal data can possibly concern the following categories of data:

- Professional contact information
  - name,
  - job title,
  - email,
  - phone number,
  - fax,
  - address
- Subscriber information

ANNEX 2 - SUPPLIER'S INFORMATION SECURITY POLICY

Supplier is to complete the status for each area and action in the table below and to insert its security policy addressing such areas and actions.

Areas	Actions	Status (Y/N)
Authentication	Set a unique login for each user	
Authentication	Adopt a user password policy	
Authentication	Require user to change password after reset	
Authentication	Limit the number of attempts to access an account	
Authorizations on a software	Define empowerment profiles	
Authorizations on a software	Remove obsolete access permissions	
Authorizations on a software	Conduct an annual review of the authorizations	
Access and Incident Management	Plan a logging system	
Access and Incident Management	Inform users of the implementation of the logging system	
Access and Incident Management	Protect logging equipment and log information	
Authorization Management	Limit access to administrative tools and interfaces to only authorized people	
Authorization Management	Install critical updates immediately	
Authorization Management	Ensure data availability	
Website security	Use the TLS protocol and check its implementation	
Website security	Verify that no password or username passes in the URLs	
Website security	Check that user entries match what is expected	
Website security	Put a consent banner for unnecessary cookies to the service	
Business continuity	Perform regular backups	
Business continuity	Store backup media in a safe place	
Business continuity	Plan security measures for conveying backups	
Business continuity	Plan and test business continuity regularly	
Archives	Implement specific access procedures for archived data	
Archives	Destroy obsolete archives in a secure way	
Maintenance and destruction of data	Record maintenance interventions in a handrail	
Maintenance and destruction of data	Supervise by an official of the organization the interventions by third parties	
Maintenance and destruction of data	Erase data from any material before scrapping	
Frame IT Developments	Offer privacy-friendly settings to end users	
Frame IT Developments	Avoid comment areas or frame them strictly	
Frame IT Developments	Test on fictitious or anonymous data	
Cryptographic functions	Use recognized algorithms, software and libraries	

Cryptographic functions	Keep secrets and cryptographic keys secure	
Duration of the storage	Identify storage times by type of data within a single data processing	
Duration of the storage	Validate the storage periods defined with the operational staff in charge of the data processing	
Duration of the storage	Define principles for purging data whose retention period is exceeded	
Duration of the storage	Define an anonymization procedure	
Duration of the storage	Create a to-do list to delete or anonymize the data when the deletion time is exceeded (privacy by default).	
Rights of person	Ensure that each type of data subject can have the information to contact the DPO.	
Rights of person	Define a procedure for the exercise of the requests of rights of persons	
Purge	Set up a purge script	

ANNEX 3 - DATA TRANSFER STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses pursuant to European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in non-European Union countries without an adequate level of data protection.

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in non-European Union countries without an adequate level of data protection.

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 Customer ("Data Exporter") to the Supplier ("Data Importer") of the personal data specified in Annex 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 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.

[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.

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***[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 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

[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.

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.

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[3]. 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.

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.

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the Data Exporter and the Data Importer under this Decision.