Customer EU Data Processing Addendum

This Data Processing Addendum ("**DPA**"), dated as of _____ __, 2018 (the "**Effective Date**"), is made to and a part of the Master Solutions Agreement, dated as of _____, 20___, as amended and supplemented from time to time (the "**Agreement**"), by and between [Enter SAI Global Entity here] a _____ *corporation* ("**Supplier**") and [Enter Customer Name here], a _____ corporation ("**Customer**"). All capitalised terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"**Agreement**" has the meaning set forth in the introductory section.

"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" will be construed accordingly.

"**Controller**" means an entity that, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"**Customer Data**" means any Personal Data that Supplier Processes on behalf of Customer in the course of providing Services.

"**Data Protection Laws**" means all effective data protection and privacy laws applicable to the Processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

"**EU Data Protection Law**" means (i) prior to May 25, 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**"); (ii) on and after May 25, 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation, or "**GDPR**").

"**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"Model Clauses" means the Standard Contractual Clauses for Processors as approved by the European Commission, attached hereto as Schedule 2.

"**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "**Process**", "**Processes**" and "**Processed**" will be construed accordingly.

"**Processor**" means an entity that processes Personal Data on behalf of a Controller.

"**Services**" means any product or service provided by Supplier to Customer pursuant to the Agreement.

"**Sub-processor**" means a third party engaged by Supplier to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

2. Scope of this DPA

This DPA applies where and only to the extent that Supplier Processes Customer Data that originates from the EEA or that is otherwise subject to EU Data Protection Law on behalf of Customer in the course of providing Services to the Customer.

3. Roles and Scope of Processing

3.1 **Role of the Parties**. As between Supplier and Customer, Customer is the Controller of Customer Data, and Supplier shall Process Customer Data only as a Processor acting on behalf of Customer.

3.2 **Customer Processing of Customer Data**. Customer agrees that (i) it will comply with its obligations as a Controller under Data Protection Laws in respect of its Processing of Customer Data and any Processing instructions it issues to Supplier; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Data Protection Laws for Supplier to Process Customer Data pursuant to the Agreement and this DPA.

3.3 **Supplier Processing of Customer Data**. Supplier will Process Customer Data only for the purposes described in this DPA and only in accordance with Customer’s documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer’s complete and final instructions to Supplier in relation to the Processing of Customer Data and Processing outside the scope of these instructions (if any) will require prior written agreement between Customer and Supplier.

3.4 Details of Processing

As defined in the SAI Global DPA Schedule 1 which is incorporated herein by this reference.

3.5 **Exceptions**. Notwithstanding anything to the contrary in the Agreement (including this DPA), the Customer acknowledges that Supplier shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes such as billing, account management, technical support, product development and sales and marketing. To the extent any such data used solely for Supplier's business purposes is considered Personal Data under Data Protection Laws, Supplier is the Controller of such data and accordingly warrants that it shall process such data in accordance with the Supplier's privacy policy and Data Protection Laws.

4. Sub-processing

4.1 **Authorized Sub-processors**. Customer agrees that Supplier may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by Supplier and authorized by Customer are listed in Schedule 1 hereto, which is incorporated herein by this reference.

4.2 Sub-processor Obligations. Supplier will: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Supplier to breach any of its obligations under this DPA.

4.3 **Changes to Sub-processors**. Supplier shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email will suffice) if it adds or removes Sub-processors at least ten (10) calendar days' prior to any such changes. Customer may object in writing to Supplier's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection.

5. Security

5.1 **Security Measures**. Supplier shall maintain an information security program that complies with applicable privacy laws and is consistent with standard practices and security standards in Supplier's industry, such as those published by the International Standards Association (ISO 27001:2013) and the National Institute of Standards and Technology (NIST). Such program shall include appropriate administrative, technical, physical, organizational, and operational safeguards and other security measures to maintain the security and confidentiality of Personal Data and to protect it from known or reasonably anticipated threats or hazards to its security and integrity. Supplier will review its information security program at least annually, or after significant changes occur, to ensure its continuing compliance, suitability, adequacy and effectiveness.

5.2 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by Supplier relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Supplier may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

5.3 **Personnel**. Supplier will ensure that any person who is authorized by Supplier to Process Customer Data (including its staff, agents and authorized Sub-processors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty). Further, Supplier shall take steps to ensure that any person who is authorized by Supplier to have access to Customer Data does not Process such data except on instructions from Customer, unless such person is required to Process such data by applicable EU Data Protection Law.

5.4 **Customer Responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service.

5.5 **Personal Data Breach Response**. Upon becoming aware of a Personal Data Breach, Supplier shall notify Customer without undue delay and will provide timely information relating to the Personal Data Breach as it becomes known or as is reasonably requested by Customer. Supplier shall promptly take reasonable steps to mitigate and, where possible, to remedy the effects of any Personal Data Breach.

6. Audits and Certifications

6.1 Customer acknowledges that Supplier is regularly audited against International standards, by independent third party auditors subject to control objectives based on guidance from the Information Technology Governance Institute, and has obtained ISO 27001:2013 certification for its Global Hosting services. Upon reasonable written request, Supplier shall supply a summary copy of its audit and certification report(s) ("**Report**") to Customer, which Reports shall be subject to the confidentiality provisions of any non-disclosure agreement provided by Supplier for Customer's execution in connection with the Reports. Supplier shall also respond to any written audit questions submitted to it by Customer provided that Customer shall not exercise this right more often than once per twelve (12) months unless following a Breach.

7. International Transfers

7.1 **DataCenter Locations**. Supplier may transfer and Process Customer Data anywhere in the world, where the Supplier, its Affiliates or its Sub-processors maintain Processing operations. The primary processing location and additional locations where personal data may be processed or viewed is detailed in Schedule 1 of this agreement. Supplier will at all times provide an

adequate level of protection for the Customer Data Processed, in accordance with the requirements of Data Protection Laws.

7.2 **Model Clauses**. To the extent that Supplier Processes any Customer Data that is protected by EU Data Protection Law or that originates from the EEA in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that Supplier shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by complying with the Model Clauses in Schedule 2 to this agreement which is incorporated herein by this reference. Supplier agrees that it is a "data importer" and Customer is the "data exporter" under the Model Clauses (notwithstanding that Customer may be an entity located outside of the EEA).

8. Return or Deletion of Data

8.1 Upon termination or expiration of the Agreement, Supplier shall (at Customer's election) return or to the fullest extent technically feasible delete all Customer Data in its possession or control. This requirement shall not apply to the extent Supplier is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Supplier shall securely isolate and protect from any further Processing, except to the extent required by applicable law.

9. Data Subject requests

9.1 To the extent permitted by law, Supplier will inform the customer without undue delay of requests from Data Subjects exercising their Data Subject rights (e.g. rectification, deletion and blocking of data) addressed directly to Supplier regarding Customer Personal Data. The Supplier at no time will communicate directly with the Data Subject.

9.2 If the customer is obliged to provide information regarding the customers Personal Data to Other Controllers or third parties (e.g. Data Subjects or the Supervisory Authority),the Supplier has, in some services, provided the Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, the Supplier shall assist the customer in doing so by providing all required information. If the customer or other Controllers are obliged to provide information about the processing of the customers Personal Data to a Data Subject, Supplier shall assist the customer in making the required information available.

10. Cooperation

10.1 If a law enforcement agency or government body sends Supplier a demand for Customer Data, Supplier will attempt to redirect the law enforcement agency

to request that data directly from Customer. As part of this effort, Supplier may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency or government body, then Supplier will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Supplier is legally prohibited from doing so.

10.2 To the extent Supplier is required under EU Data Protection Law, Supplier shall provide requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

11. General

11.1 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. Any claims against Supplier or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. Customer further agrees that any regulatory penalties incurred by Supplier in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Supplier's liability under the Agreement as if it were liability to the Customer under the Agreement.

11.2 No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

11.3 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

11.4 The parties agree that this DPA shall replace any existing DPA (including the Model Clauses (as applicable)) the parties may have previously entered into in connection with the Services.

11.5 This DPA and the Model Clauses will terminate simultaneously and automatically with the termination or expiration of the Agreement; provided, however, provisions requiring secure destruction of Personal Data and retention of Personal Data to satisfy legal or regulatory requirements shall survive the termination or expiration of the DPA for the minimum time required to satisfy the respective obligations under those provisions.

11.6 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

11.7 The Schedules to this DPA are incorporated in this DPA by this reference. If there is any conflict between this DPA and any Schedules to this DPA, the terms of this DPA shall prevail to the extent of that conflict.

11.8 The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative effective as of the Effective Date:

SUPPLIER:	**CUSTOMER:**
.....	.....
By:	By:
Name:	Name: .....
Title:	Title: .....

Schedule 1 - Processing

This Data Processing Schedule (DP Schedule) specifies for the Product(s) and Service(s) delivered by SAI Global.

1. Processing

Processing of customer provided data and files to provide Integrated Risk Management services.

1.1 Duration of Processing

For the term of the Agreement.

1.2 Processing Activities

Depending on the product(s) selected above the following list defines the processing activities with regards to Customer Personal Data:

- *Copies*
- *Deletes*
- *Links*
- *Reads*
- *Receives*
- *Sends*
- *Shares*
- *Stores*
- *Transforms*
- *Transitions*
- *Updates*

2. Categories of Data Subjects

Depending on the product(s) selected above the following list defines the Categories of Data Subjects:

- *Customer's employees (including temporary or casual workers, volunteers, assignees, trainees, retirees, pre-hires and applicants)*
- *Customer's affiliates employees (including temporary or casual workers, volunteers, assignees, trainees, retirees, pre-hires and applicants)*
- *Customer's (potential) customers (if those (potential) customers are individuals*
- *Employees of Customer's (potential) customers*
- *Customer's business partners (if those business partners are individuals)*
- *Employees of Customer's business partners*
- *Customer's visitors*
- *Customer's suppliers and subcontractors (if those suppliers and subcontractors are individuals)*
- *Employees of Customer's suppliers and subcontractors*

- *Customer's agents, consultants and other professional experts (contractors)*

3. Types of Personal Data

Depending on the product(s) selected above the following list sets out what Types of Customer Personal Data that can be processed:

- *Capabilities and Qualifications of the Individual*
  - *Education and Professional Certifications*
  - *Profession and Employment Information*
  - *Professional Affiliations*
- *Characteristics of the Individual*
  - *Demographic*
  - *Economic and Financial*
- *Habits and Activities of the Individual*
  - *Behavior*
- *Identity of the Individual*
  - *Government Identities*
  - *Identification Number*
  - *Individual*
  - *Nationality and Citizenship*
  - *Online Access and Authentication Credentials*
  - *Online Connection and Network Connectivity Data*
  - *Online Identifier*
  - *Person Name*
  - *Technology Identifiers*
  - *Telephony*
  - *Location of the Individual*
  - *Appointments, Schedules, Calendar Entries*
  - *Environment of the Individual*
  - *Physical Location of the Individual*

4. Special Categories of Personal Data

The following list sets out what Special Categories of Customer Personal Data generally can be processed.

- *None*

5. Customer obligations

5.1 Given the nature of the Products(s) and Service(s), Customer acknowledges that SAI Global is not able to verify or maintain the above Categories of Data Subjects, Type of Personal Data. Therefore, Customer will notify SAI Global about any changes to above by email to the assigned SAI Global representative. SAI Global will process Personal Data of all Data Subjects in accordance with the Agreement. If any changes require variation to the agreed Processing, Customer shall provide Additional Instructions to SAI Global.

5.2 In the absence of other instructions from Customer, SAI Global will assume that during the Service(s) it can have access, even incidentally, to all types of data provided by Customer, which data may include all Types of Personal Data and Special Categories of Personal Data. SAI Global has put in place its own technical and organization measures to safeguard all Customer Types of Personal Data, as set out within this DP Schedule.

6. Subprocessors

SAI Global may use the following Subprocessor(s) in the Processing of Customer Personal Data:

SAI Global companies located in the European Economic Area or countries considered by the European Commission to have adequate protection.

Name of Subprocessor	Address of Subprocessor
SAI Global Compliance Limited	Partis House Davy Avenue, Knowlhill, Milton Keynes, England MK5 8HJ

Commented [A1]: Only relevant for German Order Form

a. Third Party Subprocessors located in the European Economic Area or countries considered by the European Commission to have adequate protection.

Name of Subprocessor	Country in which Subprocessor is located
Amazon Web Services (only for AWS hosted services).	Germany
IBM Terramark (only for UK hosted services)	Netherlands

b. SAI Global Data Importers (SAI Global companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection)

Name of SAI Global Data Importer	Address of SAI Global Data Importer
SAI Global Compliance Inc.	United States of America
Anstat Pty Limited	Australia

Commented [A2]: For European Order Forms only

c. Third Party Data Importer (non-SAI Global companies established outside either the European Economic Area or countries considered by the European Commission to have adequate protection).

Name of Third Party Data Importer	Country in which Third Party Data Importer is located
IBM Terramark (only for US hosted services)	United States of America
Salesforce	United States of America

SAI Global will notify Customer of any intended changes to Subprocessors as follows: the assigned SAI Global representative will notify Customer by email.

7. Data Privacy Officer and Other Controllers

Customer is responsible for providing complete, accurate and up-to-date information about its data privacy officer and each other Controllers (including their data privacy officer) by email to the assigned SAI Global representative.

8. SAI Global Privacy Contact

The SAI Global privacy contact can be contacted at;

DataProtection.Officer@SAIGlobal.com

Schedule 2 - Model Clauses

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
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: [Enter customer name here].....
Address: .....

Tel.:.....; fax:..... ;e-mail: .....;

Other information needed to identify the organisation:

.....
(the data **exporter**)

And

Name of the data importing organisation: [Enter SAI Global Entity here] .....

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 Schedule 1 (as outlined in DPA section 3.4 above).

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.

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.

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.