



## Data Processing Terms and Conditions

These Data Processing Terms and Conditions ("Terms and Conditions") are offered by the Veritas entity which is the contracting party to the applicable Veritas agreement(s) in effect between Veritas and Customer under which Customer procures, and Veritas provides Services (collectively and individually, the "Agreement") and outlines terms in relation to transfers of Customer Personal Data outside the European Economic Area ("EEA") offered by Veritas Technologies LLC ("Customer Data Transfer Agreement").

The parties to the Agreement agree that the following terms shall apply to the processing of Customer Personal Data under the Agreement from the 25<sup>th</sup> May 2018:

### 1. DEFINITIONS AND

**INTERPRETATIONS:** In these Terms and Conditions:

**"Affiliate"** means an entity controlled by, under common control with, or controlling a party, where control is denoted by having, (directly or indirectly), fifty percent (50%) or more of the voting power (or equivalent) of the applicable entity;

**"Appropriate Technical and Organisational Measures"** shall be interpreted in accordance with the requirements of the Data Protection Legislation;

**"BCRPs"** means an inter-company agreement and the associated policies and procedures referred to and listed in that document which form Veritas's Binding Corporate Rules for Processors as developed, amended or updated by Veritas or Veritas Companies from time to time in accordance with the applicable Working Documents adopted by the Article 29 Working Party or applicable Data Protection Legislation. A copy of the BCRPs, when adopted and approved by relevant Supervisory Authorities will be made available at [www.veritas.com/privacy](http://www.veritas.com/privacy);

**"Customer Personal Data"** means any Personal Data the Processing of which is subject to the Data Protection Legislation, that is controlled by Customer and its Affiliates and is Processed by Veritas whilst fulfilling its obligations under the Agreement, wherever the Processing takes place;

**"Data Controller", "Data Processor", "Data Subject", and "Supervisory Authority"** shall be interpreted in accordance with the definitions in the Data Protection Legislation;

**"Data Protection Legislation"** means the General Data Protection Regulation (EU) 2016/679 ("GDPR") and all other applicable laws relating to the processing of personal data and privacy that may exist in the European Economic Area or Switzerland or United Kingdom (following Brexit) and any legislation and/or regulation implementing or made pursuant to it, or which amends, replaces, re-enacts or consolidates it;

**"Data Processing Terms"** means the terms in the existing Agreement that apply to the Processing of Customer Personal Data;

**"Personal Data"** shall be interpreted in accordance with the definitions in the Data Protection Legislation;

**"Processing"** shall be interpreted in accordance with the definitions in the Data Protection Legislation;

**"Sensitive Personal Data"** has the same meaning as 'special categories of data' in Data Protection Legislation; **"Veritas Companies"** means the members of the Veritas Group that have entered into the BCRPs;

**"Service"** means any service that Veritas undertakes for the Customer under the Agreement that involves the Processing of Customer Personal Data.

### 2. SCOPE

- a. Customer shall be the Data Controller and Veritas shall be the Data Processor in relation to the Customer Personal Data.
- b. The subject-matter of the data Processing is the performance of Veritas's obligations under the Agreement and the Processing will be carried out until the date that those obligations cease. The nature and purpose of the Processing, the types of Customer Personal Data that Veritas Processes and the categories of Data Subjects whose Personal Data is Processed is set out for each Service that Veritas provides, at [www.veritas.com/privacy](http://www.veritas.com/privacy).

- c. Customer warrants that the instructions it provides to Veritas in relation to the Processing of the Customer Personal Data will comply with the Data Protection Legislation and that its Processing of Customer Personal Data complies with the Data Protection Legislation.

### 3. PROCESSOR OBLIGATIONS

Veritas will:

- a. Process the Customer Personal Data only in accordance with written instructions from Customer (which may be specific instructions or instructions of a general nature as set out in the Agreement or as otherwise notified by Customer to Veritas in writing from time to time) and not for its own purposes. If required to Process Customer Personal Data for any other purpose by European Union or Member State law to which Veritas is subject, Veritas shall inform the Customer of this requirement before the Processing commences unless that law prohibits this on important grounds of public interest. Customer accepts that if it instructs Veritas to do something that exceeds the instructions specifically established in the Agreement, Veritas may require a reasonable additional charge to fulfil those instructions which will be as agreed in writing between the parties.
- b. at Customer's request and cost, taking into account the nature of the Processing:
  - i. assist Customer by taking Appropriate Technical and Organisational Measures and in so far as it is possible, in fulfilling Customer's obligations to respond to requests from Data Subjects of Customer Personal Data exercising their rights (to the extent that the Customer Personal Data is not accessible to the Customer through the Service); and
  - ii. taking into account the information available to Veritas assist the Customer in ensuring Customer's compliance with the obligations pursuant to Articles 32 to 36 of the GDPR or equivalent provisions in the Data Protection Legislation;
- c. implement and maintain Appropriate Technical and Organisational Measures to protect the Customer Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction, damage or theft of the Customer Personal Data and having regard to the nature of the Customer Personal Data which is to be protected. As a minimum, these will include the requirements required under the Data Protection Legislation. The specific Technical and Organisational Measures applicable to each particular Service can be found at [www.veritas.com/privacy](http://www.veritas.com/privacy);
- d. ensure that only personnel who are contractually bound to respect the confidentiality of the Customer Personal Data have access to it;
- e. not retain any of the Customer Personal Data for longer than is necessary to perform its obligations under the Agreement and, at the end of the Service or upon Customer's request, securely delete or return such Customer Personal Data to Customer in accordance with any relevant terms in the Agreement unless European Union or Member State law requires storage of the Customer Personal Data, and ensure that all Veritas Companies that have received relevant Customer Personal Data are made aware of any request to delete or return the relevant Customer Personal Data; and
- f. upon request by the Customer, update, correct or delete any Customer Personal Data, unless Customer has the ability to carry out that action on the Customer Personal Data itself, or European Union or Member State law requires storage of the Customer Personal Data, and ensure that all Veritas Companies that have received relevant Customer Personal Data are made aware of any request to update, correct, or delete the relevant Customer Personal Data.

### 4. SUB-PROCESSING

- a. Customer agrees that Veritas may transfer Customer Personal Data to Veritas Companies and the third parties listed at [www.veritas.com/privacy](http://www.veritas.com/privacy) as sub-processors for the relevant Service ("**Sub-processors**"), for the purpose of fulfilling Veritas' obligations under the Agreement. Veritas will ensure that any Sub-processors to whom Veritas transfers Customer Personal Data enter into written agreements requiring that the Sub-processor abide by provisions that are no less protective than these Terms and Conditions. Veritas will remain fully responsible to Customer for the fulfilment of its obligations under these Terms and Conditions and the Agreement. Veritas can at any time and at its discretion appoint a new Sub-processor provided that Customer is given at least fifteen (15) days' prior notice ("**Sub-processor Notice**"). If Customer has a legitimate objection to the Sub-processor, consisting of reasonable and documented grounds relating to a Sub-processor's non-compliance with applicable Data Protection Legislation, Customer may, by providing written notice to Veritas within fifteen (15) days of Veritas providing the Sub-processor Notice,

terminate the Service for which Veritas intends to use the objected-to Sub-processor. Veritas will refund Customer any prepaid fees covering the remainder of the term of such Service following the effective date of termination.

- b. In order to receive Sub-processor Notices for an Service, it shall be the responsibility of Customer to email Veritas at [Privacy@veritas.com](mailto:Privacy@veritas.com) with "Sub-processor Subscribe" in the subject line of the email, giving details of the Service for which Sub-processor Notices are required. It is also Customer's responsibility to notify Veritas of any changes to the email address to which Sub-processor Notices should be sent, using the same email address and subject line. Sub-processor Notices shall be sent to the email address from which the communication is sent, unless another email address for receipt of Sub-processor Notices is stipulated in the relevant email.

## 5. BREACH NOTIFICATION

Veritas shall notify Customer without undue delay if Veritas becomes aware of any accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to the Customer Personal Data (a "**Data Breach**"), take such reasonable steps as may be required to remedy the Data Breach and as soon as possible, provide Customer with:

- a. a detailed description of the Data Breach;
- b. the type of Customer Personal Data that was the subject of the Data Breach;
- c. the identity of each affected person, as soon as such information can reasonably be collected or otherwise becomes available as well as periodic updates to this information; and
- d. any other information Customer may reasonably request relating to the Data Breach.

## 6. DATA TRANSFERS

- a. Veritas may transfer Customer Personal Data outside the EEA, the United Kingdom (following Brexit) and Switzerland where such transfers are normally carried out for the purposes of fulfilling Veritas' obligations under the Agreement. As the data importer in relation to such transfers, Veritas Technologies LLC will comply with the obligations of a data importer as set out in the Standard Contractual Clauses for the transfer of Personal Data to data processors established in third countries adopted by the European Commission decision of 5 February 2010, published under document number C(2010) 593 2010/87/EU (the '**Standard Contractual Clauses**'), as incorporated into the Customer Data Transfer Agreement, a copy of which is at Schedule 1 hereto ("**Customer Data Transfer Agreement**"). Where the contracting party to the Agreement is a Veritas entity other than Veritas Technologies LLC, Customer hereby authorises Veritas to enter into an agreement with Veritas Technologies LLC on the terms of Customer Data Transfer Agreement as agent for Customer and Veritas agrees to enter into such agreement with Veritas Technologies LLC forthwith. The relevant Annexes 1 and 2 to the Customer Data Transfer Agreement for the Service in question, are to be found at [www.veritas.com/privacy](http://www.veritas.com/privacy). Notwithstanding the foregoing, at the point at which the Veritas Companies adopt approved BCRPs or an alternative compliance standard for the lawful transfer of Customer Personal Data, the terms of the Customer Data Transfer Agreement shall cease to apply to the transfers made pursuant to the Agreement and such transfers shall be made in accordance with Clause 6 (c) below.
- b. If the parties are relying on the Customer Data Transfer Agreement to transfer Customer Personal Data outside the EEA, and the European Commission decision on Standard Contractual Clauses is held to be invalid, or if any Supervisory Authority requires transfers of Customer Personal Data made pursuant to such decision to be suspended, then Customer may, at its discretion, require Veritas to cease processing Customer Personal Data to which this paragraph applies, or co-operate with Veritas to facilitate use of an alternative transfer, mechanism. Customer accepts that if it instructs Veritas to cease processing the Customer Personal Data, such instruction may render it impossible for Veritas to continue to provide the relevant Service or render it impossible for the Customer to continue use of the relevant Service, and if that happens, such situation shall be treated as an event beyond Veritas' reasonable control, and shall be handled in accordance with the relevant provisions in the Agreement.
- c. When the Veritas Companies adopt approved BCRPs:
  - i. Veritas (and any other Veritas Company that Customer authorises to Process Customer Personal Data in accordance with paragraph 5 of these Terms and Conditions) may transfer Customer Personal Data outside the EEA and Switzerland in accordance with the BCRPs where such transfers are normally carried out for the purposes of fulfilling Veritas' obligations under the Agreement.
  - ii. In the event, and to the extent only, of any conflict or inconsistency between the BCRPs and the provisions of these Terms and Conditions, the BCRPs shall prevail. The BCRPs shall be

binding to the Customer by means of the third-party rights set out in the BCRPs.

iii. Customer shall:

1. ensure that if the transfer involves Sensitive Personal Data, that Data Subjects have been informed of the transfer, or will be informed before the transfer, that Personal Data relating to them could be transmitted to a third country not providing adequate protection;
  2. inform Data Subjects about the existence of Data Processors outside of the EEA or Switzerland and of the BCRPs; and
  3. make available to Data Subjects upon request:
  4. a document including all the information about the BCRPs that is required by the Article 29 Working Party's Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (WP195) (a copy of which Veritas may make available for customers' use at [www.veritas.com/privacy](http://www.veritas.com/privacy)); and
  5. a copy of these Terms and Conditions, with any sensitive and confidential commercial information removed.
- iv. Veritas may modify or supplement these Terms and Conditions by notice to Customer if Veritas determines, in its sole discretion, that such modifications or additional terms are necessary for the approved and adopted BCRPs to apply to transfers of Personal Data pursuant to the Agreement.

## **7. AUDIT**

During the term of the Agreement, Veritas will allow, on at least 30 business days' notice (unless shorter notice period is required by applicable law or statutory authority), Customer and its respective auditors or authorised agents to conduct reasonable audits or inspections to verify that Veritas is processing Customer Personal Data in accordance with its obligations under the Agreement and applicable Data Protection Legislation. The scope of the audit is to be pre-agreed between the parties and such audit may include providing reasonable access within normal business hours to the premises, resources and personnel that Veritas use for the Processing of the Customer Personal Data, and Veritas will provide reasonable assistance to assist Customer in exercising its audit rights under this Section. Veritas may in certain circumstances provide a third-party audit report rather than permitting Customer itself to audit, where necessary to protect the Personal Data controlled by other customers. Veritas shall notify Customer immediately if it considers that an instruction from Customer is in breach of Data Protection Legislation, and Veritas shall be entitled but not obliged to suspend execution of the instructions concerned, until Customer confirms such instructions in writing.

## **8. MISCELLANEOUS**

- a. In the event of any conflict or inconsistency between the provisions of the Agreement and these Terms and Conditions, the provisions of these Terms and Conditions shall prevail. Save as specifically modified and amended in these Terms and Conditions, all the terms, provisions and requirements contained in the Agreement shall remain in full force and effect and govern these Terms and Conditions.
- b. Except in relation to the Customer Data Transfer Agreement, these Terms and Conditions and any dispute or claim (including non-contractual disputes or claims) arising out of, or in connection with them or their subject matter or formation shall be governed by and interpreted in accordance with the law which governs the Agreement, and Veritas and Customer irrevocably agree that the courts that have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arises out of, or in connection with, the Agreement, or its subject matter or formation, shall also have exclusive jurisdiction in relation to any disputes or claims arising from these Terms or Conditions.

## **SCHEDULE ONE**

### **CUSTOMER DATA TRANSFER AGREEMENT**

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,

**CUSTOMER** ("data exporter") and

**VERITAS TECHNOLOGIES LLC**, of 500 East Middlefield Road, Mountain View, CA 94043, United States, telephone + 1 866 837 4827 ("data importer")

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 the applicable Annex 1 and 2 for the relevant Service, a copy of which can be found at [www.veritas.com/privacy](http://www.veritas.com/privacy). The Clauses shall apply exclusively to the processing of personal data controlled by Customer that is subject to applicable laws relating to the processing of personal data and privacy that may exist in the European Economic Area or Switzerland and any legislation and/or regulation implementing or made pursuant to it, or which amends, replaces, re-enacts or consolidates them

#### **1. DEFINITIONS**

For the purposes of the Clauses:

- (a) "agreement" means the services agreement under the which the Service which requires the transfer of personal data is provided;
- (b) "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;
- (c) the "data exporter" means the controller who transfers the personal data;
- (d) the "data importer" means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its 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;
- (e) the "sub-processor" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;
- (f) 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;
- (g) "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.

#### **2. DETAILS OF THE TRANSFER**

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

#### **3. THIRD-PARTY BENEFICIARY CLAUSE**

- 3.1 The data subject can enforce against the data exporter this clause 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.
- 3.2 The data subject can enforce against the data importer this clause 3.2, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 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.
- 3.3 The data subject can enforce against the sub-processor this clause 3.3, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 3.4 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.

#### **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 the relevant Annex 2 for the Services;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to clause 5(b) and clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of the relevant Annex 2 for the Services and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and

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

## **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 the relevant Annex 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
  - (ii) any accidental or unauthorised access; and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with clause 11; and
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

## **6. LIABILITY**

- 6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
- 6.2 If a data subject is not able to bring a claim for compensation in accordance with clause 6.1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in clause 3 or in clause 11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if

it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

- 6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in clauses 6.1 and 6.2, arising out of a breach by the sub-processor of any of their obligations referred to in clause 3 or in clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 6.4 Nothing in these conditions excludes or limits the liability of the data importer to a data subject hereunder under Clause 6.2 above.
- 6.5 The data importer's total liability arising in connection with the performance or contemplated performance of the Clauses shall be limited to the amount specified in the limitation of liability clause in the agreement, or where the contracting party to the agreement is a Veritas entity other than the data importer, the liability of both the data importer and the contracting Veritas entity in aggregate shall be limited to the amount specified in the limitation of liability clause in the agreement with that contracting Veritas party.

## **7. MEDIATION AND JURISDICTION**

- 7.1 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.
- 7.2 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.

## **8. COOPERATION WITH SUPERVISORY AUTHORITIES**

- 8.1 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.
- 8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
- 8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to clause 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

## **9. GOVERNING LAW**

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

## **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 Clauses.



## **11. SUB-PROCESSING**

- 11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
- 11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in clause 6.1 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in clause 6.1 shall be governed by the law of the Member State in which the data exporter is established.
- 11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## **12. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES**

- 12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
- 12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in clause 12.1.

## **13. TERMINATION**

Should data importer and its group of companies adopt approved Binding Corporate Rules for Processors ("BCRPs"), the terms of this Veritas Customer Data Transfer Agreement shall cease to apply to the relevant transfers of personal data made hereunder, and such transfers shall automatically be deemed to be made subject to the BCRPs instead.