VERITAS™

DATA PROCESSING TERMS FOR PROVIDERS

These Data Processing Terms form part of the Agreement between Provider and Veritas (as defined below) where the supply of the Services involves the Processing of Personal Data, and/or EU Personal Data (as defined below).

1. The following terms shall apply to processing of all Personal Data regardless of its origin or the applicable law:

   1.1. Provider shall comply with all applicable laws, rules, regulations and other legal requirements relating to (a) privacy, data security, and protection of Personal Data; and (b) the Processing of any Personal Data.

   1.2. Provider shall process Personal Data only in compliance with Veritas' written instructions (which may be specific instructions or instructions of a general nature as set out in the SOW, the underlying Agreement or as communicated by Veritas from time to time) and not for any other purpose.

   1.3. Provider shall not retain any of the Personal Data for longer than is necessary to perform the obligations under the Agreement or applicable SOW, and at the end of the Services upon Veritas' request, return or securely destroy such Personal Data.

   1.4. Provider shall process Personal Data at the locations agreed upon in the Agreement or applicable SOW and shall not transfer Personal Data across country borders unless expressly authorized in writing by Veritas.

   1.5. When Personal Data is collected on behalf of Veritas, if such collection is permitted or required to be done in a situation where Provider displays or communicates the Veritas name or logo to the public, Provider shall ensure that it obtains an agreed privacy notice from Veritas, and that this is presented at the time of collection. Provider warrants it has the required consent from the Data Subject to ensure such Personal Data is collected and subsequently used by Veritas in accordance with applicable privacy and data protection laws. Provider will also comply with Veritas' reasonable requests to support its legal and/or contractual obligations to provide Individuals with access to Personal Data under applicable privacy and data protection laws.

   1.6. In the event of any actual or reasonably suspected unauthorized access, use, disclosure, tampering, destruction or loss of Personal Data, Provider will provide Veritas (or an independent third party designated by Veritas) with access to its premises and systems for the purposes of investigating the breach, upon 48 hours advance notice. Provider shall notify affected Individuals or regulatory authorities where required by applicable law or requested by Veritas, and will take such steps as deemed necessary by Veritas to protect affected Individuals from fraud or identity theft as is necessary, including but not limited to making credit reports or watch facilities available, reimbursing Veritas and holding it harmless for any cost related to notifications and, where applicable, for the costs of providing credit reporting and/or monitoring services for Individuals actually or potentially affected.

   1.7. Provider shall inform and train its Personnel who are responsible for handling and protecting Personal Data about privacy laws and regulations, and about the obligation to protect Personal Data in accordance with the requirements of this Agreement.

2. The following terms shall apply to the Processing of EU Personal Data as defined below, in addition to the terms in section 1 above. Where there is a conflict between the terms of this section 2, and the terms of section 1, the terms of this section 2 shall prevail in relation to EU Personal Data.

DEFINITIONS

   2.1. In this section 2 to the Data Processing Terms:

   "**BCRPs**" means Veritas's Binding Corporate Rules for Processors as developed, amended or updated by Veritas from time to time, a copy of which, when adopted and approved by relevant Supervisory

Authorities will be made available at www.veritas.com/privacy;

"**Data Controller**", "**Data Processor**", "**Data Subject**", **"Personal Data"**, "**Processing**" and "**Appropriate Technical and Organisational Measures**" and **"Supervisory Authority"** shall be interpreted in accordance with the Data Protection Legislation;

"**Data Protection Legislation**" means the GDPR and all other applicable laws relating to Processing of Personal Data and privacy that may exist in the EEA, the United Kingdom or Switzerland and any legislation and/or regulation made pursuant to it, or which amends, replaces, re-enacts or consolidates it;

"EEA" means the European Economic Area;

"EU Personal Data" means any Personal Data the Processing of which is subject to Data Protection Legislation, that is controlled by Veritas and its Affiliates and their respective customers (where applicable), which Provider Processes when providing the Services under the Agreement, wherever the Processing takes place;

"GDPR" means the General Data Protection Regulation (EU) 2016/679;

"**Veritas**" means the entity within the Veritas group of companies that is the Veritas contracting party to the Agreement, acting for itself and for and on behalf of its Affiliates and customers in the EEA, the UK and Switzerland that are Data Controllers of EU Personal Data;

DATA PROTECTION

2.2 Provider agrees that Veritas, and its Affiliates and customers located in the EEA, the United Kingdom and Switzerland, are the Data Controllers and Provider is the Data Processor in relation to the EU Personal Data. The nature and purpose of the Processing, the types of EU Personal Data Provider Processes and the categories of Data Subjects whose EU Personal Data is Processed shall be laid out in the relevant SOW or other exhibit to the Agreement.

2.3 The subject-matter of the data Processing is the supply of the Services and the Processing will be carried out until the date that Provider ceases to provide the Services to Veritas.

2.4 When Provider Processes EU Personal Data when providing the Services, Provider will:

2.4.1 Process the EU Personal Data only in accordance with written instructions from Veritas (which may be specific instructions or instructions of a general nature as set out in these Data Processing Terms, the Agreement or as otherwise notified by Veritas to Provider from time to time) and not for Provider's own purposes. Veritas accepts that if Veritas issues a direction to Provider which requires Provider to do something that is inconsistent with the terms of the Agreement, Provider may wish to make a reasonable charge, in which case that charge will be as agreed in writing between the parties. If Provider is required to Process the EU Personal Data for any other purpose by European Union or Member State law to which Provider is subject, Provider will inform Veritas of this requirement before the Processing, unless that law prohibits this on important grounds of public interest;

2.4.2 notify Veritas immediately if, in Provider's opinion, an instruction for the Processing of EU Personal Data given by Veritas infringes applicable Data Protection Legislation;

2.4.3 taking into account the nature of the Processing, assist Veritas:

2.4.3.1 by taking Appropriate Technical and Organisational Measures and in so far as it is possible, in fulfilling Veritas's obligations to respond to requests from Data Subjects exercising their rights; and

2.4.3.2 in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR or equivalent provisions in the Data Protection Legislation;

2.4.4 implement and maintain Appropriate Technical and Organisational Measures to protect the EU 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 EU Personal Data and having regard to the nature of the EU Personal Data which is to be protected. As a minimum, these shall include the requirements required under applicable Data Protection Legislation and the "Provider Security Requirements" or other security provisions that may be agreed between Veritas and Provider, as set out in the relevant exhibit to the Agreement. Veritas may ask Provider at any time to provide, within a reasonable timescale, a written description of the technical and organisational methods Provider employs for Processing EU Personal Data;

2.4.5   not give access to or transfer any EU Personal Data to any third party (including any Affiliates, group companies or sub-contractors) without the prior written consent of Veritas. Where Veritas does consent to Provider engaging a sub-contractor to carry out any part of the provision of the Products, Provider must ensure the reliability and competence of the third party, its employees and agents who may have access to the EU Personal Data and must include in any contract with the third party, provisions in favour of Veritas which are equivalent to and no less onerous those in these Data Processing Terms and as are required by applicable Data Protection Legislation. For the avoidance of doubt, where a third party fails to fulfil its obligations under any sub-processing contract or any applicable Data Protection Legislation, Provider will remain fully liable to Veritas for the fulfilment of Provider's obligations under these Data Processing Terms and the Agreement;

2.4.6   take reasonable steps to ensure the reliability and competence of Provider personnel who have access to the EU Personal Data;

2.4.7   ensure that personnel required to access the EU Personal Data are informed of the confidential nature of the EU Personal Data and comply with the obligations set out in these Data Processing Terms;

2.4.8   ensure that none of Provider's personnel publish, disclose or divulge any of the EU Personal Data to any third party unless directed in writing to do so by Veritas;

2.4.9   not retain any of the EU Personal Data for longer than is necessary to perform Provider's obligations under the Agreement and, at the end of the supply of the Services upon Veritas's request, securely destroy or return such EU Personal Data to Veritas; and

2.4.10   allow Veritas and its respective auditors or authorised agents to conduct audits or inspections during the term of the Agreement, which will include providing access to the premises, resources and personnel Provider and Provider's sub-contractors used in the provision of the Products, and provide all reasonable assistance to assist Veritas in exercising its audit rights under these Data Processing Terms. The purposes of an audit pursuant to these Data Processing Terms include verifying that Provider is Processing EU Personal Data in accordance with Provider's obligations under these Data Processing Terms, the Agreement and applicable Data Protection Legislation.

2.5 If Provider becomes aware of any accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to the EU Personal Data that Provider Processes when providing the Services (a "**Personal Data Breach**"), Provider will:

2.5.1   notify Veritas without undue delay (and in any event within 48 hours);

2.5.2   provide Veritas (as soon as possible) with a detailed description of the Personal Data Breach, the type of EU Personal Data that was the subject of the Personal Data Breach and the identity of each affected person, as soon as such information can be collected or otherwise becomes available (as well as periodic updates to this information and any other information Veritas may reasonably request relating to the Personal Data Breach); and

2.5.3   not release or publish any filing, communication, notice, press release, or report concerning the Personal Data Breach without Veritas's prior written approval (except where required to do so by law).

2.6 If the European Commission lays down, or an applicable supervisory authority adopts, standard contractual clauses for the matters referred to in Article 28(3) and Article 28(4) of the GDPR pursuant to Article 28(7) or Article 28(8) of the GDPR (as appropriate) and Customer notifies Provider that it

wishes to incorporate any element of any such standard contractual clauses into the Agreement, Provider will agree to the changes as reasonably required by Veritas to achieve this.

2.7 Provider will not Process EU Personal Data outside the EEA, or a country in respect of a valid adequacy decision has been issued by the European Commission, except with the prior written consent of Veritas. Where Veritas gives its consent, such transfers will be made subject to the terms of 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, a copy of which is at Annex 1 hereof or any replacement or additional form approved by the European Commission or as applicable in the UK, Switzerland or Jersey.

2.8 If the European Commission decision authorising the data transfer mechanism used to legitimate the data transfers made under the Agreement is held to be invalid, or any Supervisory Authority requires transfers of EU Personal Data made pursuant to such decision to be suspended, then Veritas may, at its discretion, require Provider to cease processing EU Personal Data to which this paragraph applies, or promptly co-operate with Veritas to facilitate use of an alternative transfer mechanism.

2.9 Where the EU Personal Data is controlled by Veritas customers that transfer such EU Personal Data to Veritas acting as a Data Processor pursuant to the BCRPs rather than the Standard Contractual Clauses (each a "Veritas Customer"), Paragraphs 7.2 to 7.13 and 7.18 and 7.19 of the European Appendix to the Global Privacy Policy, which forms part of the BCRPs, shall be incorporated into this Agreement as if references to "Veritas" in the BCRPs refer to Provider, references to "Relevant Customer" are to the relevant Veritas Customer and references to "Customer Personal Information" are to EU Personal Data.

2.10 Provider shall co-operate and assist the Veritas Customer to comply with Data Protection Legislation (such as its duty to respect the Data Subject rights or to handle their complaints or to be in a position to reply to investigation or inquiry from a Supervisory Authority) within a reasonable time and to the extent reasonably possible.

2.11 Provider shall communicate claims or requests in respect of EU Personal Data without delay to Veritas to enable Veritas to provide details to the Veritas Customer and will handle complaints from Data Subjects where the Veritas Customer and Veritas or relevant Veritas Affiliates have disappeared factually or has ceased to exist in law or have become insolvent.

2.12 Provider agrees that Data Subjects have the right to enforce the provisions of these Data Processing Terms insofar as they are required to be imposed on Provider pursuant to the BCRPs as third-party beneficiaries against the Provider in a case where the Data Subject is not able to bring a claim against the relevant Veritas Customer or Veritas or the relevant Veritas Affiliate because the Veritas Customer, Veritas or the relevant Veritas Affiliate have factually disappeared or ceased to exist in law or have become insolvent. Such right shall not apply where any successor entity has assumed the entire legal obligations of the Veritas Customer or Veritas or the relevant Veritas Affiliate by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The Data Subjects' rights shall cover the judicial remedies for any breach of the rights guaranteed and the right to receive compensation for any damage (material harm but also any distress). The Data Subject may take action before the Supervisory Authority competent to enforce against Provider, or court with jurisdiction over Provider or, at Data Subject's option, the courts of the country where Data Subject is resident. If more favourable solutions for the Data Subject exist according to national law, then they shall be applicable.

3 MISCELLANEOUS

In the event of any conflict or inconsistency between the provisions of the Agreement and these Data Processing Terms, the provisions of these Data Processing Terms shall prevail to the extent that they are more stringent than those in the Agreement, unless such provisions are expressly and specifically stated to have been amended by a provision in the Agreement or relevant SOW.

Annex 1

Standard Contractual Clauses

Standard contractual clauses for the transfer of Personal Data from the Community to third countries (controller to processor transfers)

Data Transfer Agreement

Parties

This Agreement is made between:

(1)   **Veritas,** acting on its own account and for and on behalf of those of its Affiliates and customers (where applicable) that are the controllers of Personal Data,

 (hereinafter the "**data exporter**");

and

(2)   Provider

(hereinafter 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 the Agreement.

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 within the SOW or relevant exhibit to the Agreement which shall form an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

a) 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(a) and (b), Clause 7, Clause 8(b), and Clauses 9 to 12 as third-party beneficiary.

b) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(b), 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.

c) The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(b), 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.

d) 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 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 Data Processing Terms;

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(c) 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, and a summary description of the security measures, as well as a copy of any contract for subprocessing 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 the Data Processing Terms 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 the full description of the security measures in the Agreement, 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 of Personal Data 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

a)   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.

b)   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.

c)   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

d)   If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs (a) and (b), 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

a)   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:

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

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

b)   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

a)   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.

b)   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.

c)   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 (b). 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

a)   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.

b)   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 (a) 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.

c)   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph (a) shall be governed by the law of the Member State in which the data exporter is established.

d)   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

a)   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.

b)   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 (a).