



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 the processing and the transfers of Customer Personal Data outside the European Economic Area ("EEA") and United Kingdom 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 and form part of the Agreement:

1. DEFINITIONS AND INTERPRETATIONS: In these Term and Conditions (all capitalised terms not defined herein shall have the meaning set out in the Agreement):

"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;

"CCPA" means the California Consumer Privacy Act of 2018, codified at Cal. Civ. Code §1798.100 *et seq* and its implementing regulations as may be amended from time to time;

"Customer Personal Data" means any Personal Data the Processing of which is subject to the Data Protection Legislation, that is disclosed by Customer and its Affiliates to Veritas to enable Veritas to fulfil its obligations under the Agreement;

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

"Data Protection Legislation" means all applicable data protection and privacy laws, regulations and mandatory codes of practice applicable to the Processing of Customer Personal data including the General Data Protection Regulation (EU) 2016/679 ("EU GDPR") and all other laws that may exist in the European Economic Area, Switzerland or United Kingdom relating to the Processing of Personal Data and any legislation and/or regulation as amended, repealed, consolidated or replaced from time to time;

"Lawful Safeguards" means such legally enforceable mechanism(s) for transfers of Customer Personal Data as may be permitted under Data Protection Legislation from time to time;

"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;

"Sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, personal information to a third party for monetary or other valuable consideration;

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

"Veritas Companies" means the members of the Veritas Group.

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.
- 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 EU 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 and the Security Safeguards detailed in Annex II. The specific Technical and Organisational Measures applicable to each particular Service can be found at 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 for the purposes of Veritas's obligations under the Agreement;
 - 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 <https://www.veritas.com/content/dam/Veritas/docs/policies/sub-processors-for-veritas-services.pdf> 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 shall provide written notice of such objection to Veritas during the fifteen (15) days of Veritas providing the Sub-processor Notice.

- b. In order to receive Sub-processor Notices for a Service, it shall be the responsibility of Customer to email Veritas at 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 a confirmed 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 investigate and remedy the Data Breach and as soon as possible and where known by Veritas provide Customer with:

- a. a detailed description of the Data Breach as at that time and the mitigations enacted;
- b. the type and volume 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 by way of Lawful Safeguards. For transfers to third countries outside the EEA, the United Kingdom and Switzerland where such transfers are normally required 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 European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data, published under document number C(2021) 3972, (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**”).

- b. 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.
- c. 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.

7. AUDIT

- a. 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 these Terms and Conditions and applicable Data Protection Legislation.
- b. 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.
- c. Veritas may in certain circumstances provide a third-party audit report or complete questionnaires rather than permitting Customer itself to audit where Veritas believes its compliance can be verified in such a manner.
- d. 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. CCPA

Customer has made Personal Data available to Veritas. Veritas agrees that Veritas (i) will not retain, use or disclose, any Personal Data of the Customers for any purpose other than for the specific purpose of performing the Services for the Business Purposes (as defined in CCPA) of the Customer under the Agreement; and (ii) will not sell Personal Data. Veritas confirms that it understands and will comply with these obligations.

9. 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

STANDARD CONTRACTUAL CLAUSES

The Parties have agreed on the following Standard Contractual Clauses (transfer controller to processor- Module 2) (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 personal data specified in the attached Annex I.

For the purposes of the Clauses, Customer is the data exporter and Veritas is the data importer.

In case of any transfer of Customer Personal Data where Data Protection Legislation of the UK apply to the data exporter's processing when making that transfer, (i) references to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws, as applicable; and (ii) any other obligation in these SCCs determined by the Member State in which the data exporter or the data subject is established shall refer to an obligation under UK Data Protection Laws, as applicable.

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)¹ for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex IA. (hereinafter each "data exporter"), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter,

¹ Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

directly or indirectly via another entity also Party to these Clauses, as listed in Annex IA. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex IB.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfers

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex IB.

Clause 7 – Optional

Docking clause

Reserved

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions

from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex IB, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex IB. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”).

In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex IB.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union^[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

[2] *The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.*

Clause 9

Use of sub-processors

- (a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the

engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

[3] *This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.*

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with

these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article **23(1)** of Regulation **(EU) 2016/679**, are not in contradiction with these Clauses.

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

 - (ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards²;

² As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully

- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request

shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

and the response provided; or

- (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV - FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) [For Modules One, Two and Three]: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.

The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): Controller

2. ...

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: Global Director of Privacy, privacy@veritas.com

Activities relevant to the data transferred under these Clauses: See section B below

Signature and date: ...

Role (controller/processor): Processor

2. ...

B. DESCRIPTION OF TRANSFER

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

- *Categories of data subjects whose personal data is transferred*

Customer may submit Personal Data to the Services, the extent to which is determined and controlled by the exporter, and which may include but is not limited to the following categories of data subjects:

Workers of the Data Exporter that are named as persons authorised to use the Services, its Affiliates and the suppliers and customers, and any other categories of individuals that correspond or interact with the Data Exporter in the course of its business.

- *Categories of personal data transferred*

Customer may submit Personal Data to the Services, the extent to which is determined and controlled by the exporter, and which may include but is not limited to the following categories of Personal Data:

First name

last name

contact information (company, email, phone, business address)

IP data

Miscellaneous categories of Personal Data that exist in the various communications and documents archived in the Service.

- *Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

Customer may submit special categories of data to the Services, the extent to which is determined and controlled by the data exporter. In the context of the processing of the Customer Data in the Service: Miscellaneous categories of Sensitive Personal Data that exist in the various communications and documents archived in the Service.

- *The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

Customer Personal Data will be transferred periodically throughout the term of the Agreement. Customer will have control over each transfer to Veritas.

- *Nature of the processing*

Performance of the Service(s) pursuant to the Agreement.

- *Purpose(s) of the data transfer and further processing*

As necessary to perform the Services pursuant to the Agreement and as further specified in the Service privacy notice available at <https://www.veritas.com/company/privacy>.

- *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

Subject to Section 3 (e) and (f) of the DPA, for the duration of the Agreement, unless otherwise agreed upon in writing.

- *For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

General authorisation for the engagement of sub-processor(s) from an agreed list available at <https://www.veritas.com/content/dam/Veritas/docs/policies/sub-processors-for-veritas-services.pdf>

C. COMPETENT SUPERVISORY AUTHORITY

Clause 13 shall apply as follows:

Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, shall act as competent supervisory authority; or

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, shall act as competent supervisory authority; or

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, The Data Protection Commission (DPC) shall act as competent supervisory authority; or

Where the data exporter is established in the United Kingdom or falls within the territorial scope of the application of UK Data Protection Legislation, the Information Commissioner's Office (ICO) shall act as competent supervisory authority.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

[Please reference those in the Master Agreement]

ANNEX III

LIST OF SUB-PROCESSORS

General authorisation for the engagement of sub-processor(s) from an agreed list available at <https://www.veritas.com/content/dam/Veritas/docs/policies/sub-processors-for-veritas-services.pdf>

