DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is entered into by and among the Symantec contracting entity as specified in the Agreement ("**Symantec**") and company identified below, on its behalf and as required, in the name and on behalf of its affiliated companies ("**Customer**").

Symantec has pre-signed this Addendum. In order for this Addendum to come into effect, Customer shall fill in the information (full legal entity name, address, name and title of signatory and date of signature) in the signature box (page 7) and return the completed and signed copy of this Addendum to privacyteam@symantec.com.

WHEREAS Customer has procured certain Services provided by Symantec that involve the Processing of Personal Data subject to Applicable EU Legislation.

WHEREAS This Addendum serves as the binding contract referred to in Article 28 (3) of the GDPR that sets out the subject-matter, duration of processing, nature and purpose of processing, the type of personal data and categories of data subjects as well as the obligations and rights of the Controller which maybe further supplemented by the terms and conditions applicable to the Services delivered by Symantec to Customer (the "**Agreement**").

WHEREAS In the provision of Services by Symantec to Customer pursuant to the Agreement, Customer acts as Controller and Symantec acts as Processor with respect to the Personal Data or as the case maybe, Customer acts as a Processor for its end user customers including such end user customers' affiliated companies (as ultimate Controllers) and Symantec will act as a Sub-Processor acting on the instruction of the Customer vis-a-vis its end user customers.

The parties agree as follows:

1. **Definitions**. Unless otherwise defined in the Agreement, all capitalized terms used in this Addendum will have the meanings given to them herein.

   "**Applicable EU Legislation**" means the: (i) 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 and, as of 25 May 2018, the then applicable General Data Protection 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, and repealing Directive 95/46/EC ("**GDPR**"); and (ii) to the extent applicable to the Services, any other EU or EU Member State data protection laws with respect to the processing of Personal Data under the Agreement.

   "**Controller**" has the meaning given to it in the Applicable EU Legislation and for the purposes of this Addendum means Customer including when acting on behalf of its end user customer.

   "Data Subject" has the meaning given to it in the Applicable EU Legislation.

   "**EEA**" means the European Economic Area.

   "**Personal Data**" has the meaning given to it in the Applicable EU Legislation and for the purpose of this Addendum relates to the personal data Processed by Symantec as described in Section 4.

   "**Personal Data Breach**" has the meaning given to it in the Applicable EU Legislation.

   "**Processing**" has the meaning given to it in the Applicable EU Legislation and "process", "processes" and "processed" will be construed accordingly.

   "**Processor**" has the meaning given to it in the Applicable EU Legislation and for the purposes of this Addendum means Symantec.

"**Services**" means the Online Service(s) and other services offered by Symantec and procured by the Customer.

"**Standard Contractual Clauses"** means the Standard Contractual Clauses pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to Processors established in third countries under the Directive set forth in Exhibit 1 to and forming part of this Addendum.

2. **Compliance with Laws**. Each party will comply with the Applicable EU Legislation as applicable to it. In particular, Customer will comply with its obligations as Controller (or on behalf of Controller) and Symantec will comply with its obligations as Processor.

3. **Customer Obligations.** Customer as Controller (or on behalf of the ultimate Controller) undertakes that all instructions for the Processing of Personal Data under the Agreement or this Addendum or as otherwise agreed or configured shall comply with Applicable EU Legislation, and such instructions will not in any way cause Symantec to be in breach of any Applicable EU Legislation. Customer is solely responsible for ensuring the accuracy, quality, and legality of Personal Data Processed by Symantec including the means by which Customer acquired Personal Data.

4. **Data Processing.** Symantec will Process the Personal Data for the sole purpose of enabling, optimizing and providing the Services and/or for the purposes specified under the Agreement and this Addendum. Symantec will Process the Personal Data as described in the table below in accordance with Customer's instructions as documented in the Agreement and this Addendum for the term of the Agreement. Symantec will not access, use or otherwise Process such Personal Data, except as necessary to provide the Services.

   Unless prohibited by applicable law, Symantec shall notify Customer if in its opinion, an instruction infringes any EU Member State law to which it is subject, in which case Symantec will be entitled to suspend performance of such instruction, until Customer confirms in writing that such instruction is valid under EU Member State law.

   Any additional instructions regarding the manner in which Symantec Processes the Personal Data will require prior written agreement between Symantec and Customer, including where applicable any additional fees to be paid by Customer.

   As part of the configuration of the Services, certain security features and data processing functionalities are made available to the Customer. Customer is responsible for properly configuring the Services to meet its specific Processing and security requirements, which may include use of pseudonymisation or encryption technology to protect the Personal Data from unauthorized access.

   Symantec will not disclose Personal Data to any government, except as necessary to comply with applicable law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). In the event that Symantec receives a binding order from a law enforcement agency for Personal Data, and provided that Symantec is not legally prohibited from doing so, Symantec will notify Customer of the request it has received.

   Symantec shall ensure that persons entrusted to process Personal Data have committed themselves to confidentiality and/or are bound by related obligations under Applicable EU Legislation or other provisions of statutory law.

Data Protection Laws **Categories of Personal Data (*)**	(a) Contact details including but not limited to name, job title and level, business email addresses and other contact details such as title, phone number and office address; (b) Email addresses, IP addresses and other network and devices or software identification information; (c) Online data (e.g. website usage, browsing activities and preferences and other web traffic data); (d) Log data which may include certain source and destination IP addresses, host name, user-ids, URLs, policy names, email addresses, date and time stamps, data volumes, email activity and content; (e) Any Personal Data which may be contained within (i) email and web communications (including their attachments) which are sent to or from employee or users of the Customer' network, (ii) any Personal Data that may be shared by Customer's employees or users with cloud applications used in the data exporters network and ; (iii)technical and support requests raised by or on behalf of Customer; and (f) Any other email and web activity related Personal Data as required for the provision of the Services.
Categories of Data Subjects (*)	Customer's employees, representatives, customers, vendors, and/or any other business contacts including senders and recipients of emails, as applicable.

(*) Complementary description of the categories of Personal Data and Data Subjects can be found at www.symantec.com

5. **Technical and organizational measures.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Symantec shall in relation to the Personal Data implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risk as further documented in Exhibit 2 of the Addendum and/or at https://www.symantec.com/about/customer-trust-portal or any successor website.

   In assessing the appropriate level of security, Symantec shall take into account in particular the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

   Customer is solely responsible for assessing whether the security measures implemented by Symantec pursuant to this Section 5 for the provision of the Services meet its own standards and requirements.

6. **Data Subjects rights.** Taking into account the nature of the Processing and the information available to Symantec, Symantec will assist Customer by appropriate technical and organisational measures, insofar this is possible, in responding to Data Subjects' requests exercising their rights under the Applicable EU Legislation. To that effect, Symantec will: (i) to the extent permitted by applicable law, promptly notify Customer of any request received directly from Data Subjects to access, correct or delete its Personal Data without responding to that request; and (ii) upon written request from Customer, provide Customer with information that Symantec has

available to reasonably assist Customer in fulfilling its obligations to respond to Data Subjects exercising their rights under the Applicable EU Legislation.

7. **Data Protection Impact Assessments**. In the event that Customer is required under Applicable EU Legislation to conduct a Data Protection Impact Assessment, then if requested to do so by Customer in writing to Symantec, Symantec will assist where reasonably possible, subject to the nature of the Processing and the information available to Symantec, in the fulfilment of the Customer's obligation as related to the Customer's use of the Services, subject to the extent Customer does not otherwise have access to the relevant information. If required under Applicable EU Legislation Symantec shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Data Protection Authorities in relation to any applicable Data Protection Impact Assessment.

8. **Audit of Technical and Organizational Measures.** Upon Customer request, Symantec agrees to make available all information necessary to demonstrate its compliance with data protection policies and procedures implemented as part of the Services. Customer is informed that Symantec conducts on a regular basis internal audits which are in accordance with industry recognized standards such as ISO 27001 or other then current relevant security certification at Symantec's sole discretion.

   Upon written request (not more than once annually) Symantec shall provide to Customer the details of the most recent audit performed by Symantec in relation to the Services. If an audit conducted by Symantec identifies security concerns considered to be high risk by industry standards, Symantec shall notify the Customer of the corrective actions implemented by Symantec to remediate such concerns and confirm in due course to Customer the return to appropriate state of compliance. If after reviewing the above mentioned information provided by Symantec, Customer has serious and substantiated reasons to believe that material security problems exist in relation to the Services, Customer may, at its sole cost and expense, verify Symantec's compliance with its data protection obligations as specified in this Addendum by: (i) submitting a security assessment questionnaire to Symantec; and (ii) if Symantec's responses to the questionnaire does not resolve the Customer's concerns, Customer may conduct an online or (if deemed necessary) on-site audit in the form of meetings with Symantec information security experts, subject to a minimum thirty (30) business days' prior written notice. Subject to the above, both parties agree that any such follow up verification will be limited to once a year and will be conducted with a minimum of disruption to Symantec's normal business operations and subject always to Symantec's agreement on scope and timings. The Customer may perform the verification described above either itself or by a mutually agreed upon third party auditor, provided that Customer or its authorized auditor executes a mutually agreed upon Non-Disclosure Agreement ("NDA"). Customer shall be responsible for any actions taken by its authorized auditor. All information disclosed by Symantec under this Section 8 shall be deemed Symantec Confidential Information and the Customer shall not disclose any audit report to any third party except as obligated by law, court order or administrative order by a government agency.

9. **Breach notification.** In the event that Symantec becomes aware of a Personal Data Breach that results in unlawful or unauthorized access, loss, disclosure, or alteration of the Personal Data Processed by Symantec as part of delivery of the Services, which is likely to cause a risk to the fundamental rights and freedoms of the Data Subjects', Symantec shall notify the Customer without undue delay after becoming aware of such Personal Data Breach and shall co-operate with the Customer and take such reasonable commercial steps as agreed with the Customer to assist in the investigation, mitigation and remediation of such Personal Data Breach. Symantec shall provide all reasonably required support and cooperation necessary to enable Customer to comply with its legal obligations in case of a Personal Data Breach pursuant to Articles 33 and 34 of the GDPR.

10. **Sub-processing.** Customer agrees that Symantec may engage either Symantec affiliated companies or third parties providers as sub-Processors under Agreement and this Addendum ("**sub-Processors**") and hereby provides Symantec with a general written authorization for the engagement of such sub-Processors in the provision of the Services. Symantec will restrict the Processing activities performed by sub-Processors to only what is strictly necessary to provide the Services to Customer pursuant to the Agreement and this Addendum. Symantec shall impose appropriate contractual obligations in writing upon the sub-Processors that are no less protective than this Addendum and Symantec will remain responsible for the sub-Processors compliance with the obligations under this Addendum.

    Symantec makes available to Customer a list of all sub-Processors used by Symantec in the provision of Services on www.symantec.com/privacy. Symantec may amend the list of sub-Processors by adding or replacing sub-Processors at any time and any material changes to the list of sub-Processors will be disclosed at the applicable location on www.symantec.com/privacy with thirty (30) business days' notice prior to any changes taking effect. Customer will be entitled to object to a new sub-Processor by notifying Symantec in writing the reasons of its objection within the above mentioned thirty (30) day notice period and in such case Customer shall have the right to terminate the applicable Services.

11. **Transfers of Personal Data to Sub-processors.** Customer acknowledges and agrees that Symantec may process Personal Data in the facilitation or provision of the Services either in the EEA and/or in countries that may have different protective data protection laws ("**Third Country/ies**"). In the event Symantec intends to transfer Personal Data to sub-Processor(s) established in a Third Country/ies and if required by the Applicable EU Legislation, Symantec shall execute on behalf of the Customer and in its capacity as data exporter, Standard Contractual Clauses in the form provided in Exhibit 1 with the sub-Processor(s) as data importer(s), unless the transfer of Personal Data occurs via an alternative means permitted by Applicable EU Legislation.

12. **Return or Deletion of Personal Data.** To the extent that the deletion of Personal Data is not specified in the Agreement, Symantec will, upon receiving Customer's written request, delete or return, as determined easiest in Symantec's sole discretion, Personal Data within a reasonable period of time to be confirmed by Symantec.

13. **Entire Agreement; Conflict.** Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

14. **Counterparts and Facsimile or Email Delivery.** This Addendum may be executed in two or more counterparts, each of which when so executed shall be deemed an original and all of which together shall constitute one and the same instrument. Signatures may be exchanged via facsimile or email transmission, each of which shall be effective as an original.

15. **Authorized Signatory**. The signatories hereto represent that they are duly authorized to sign the Addendum on behalf of their respective companies.

    Exhibit(s): Exhibit 1 – Standard Contractual Clauses

    Exhibit 2 – Description of technical and organizational measures

Agreed and Accepted as of the signature date below:

Customer Signature

Customer Name:
Signature:
Printed Name and Title:
Date Signed:

Symantec Signature

Symantec Corporation ☐ 350 Ellis Street, Mountain View CA 94043, USA	**Symantec Ltd.** ☒ Ballycoolin Business Park, Blanchardstown, Dublin 15, Ireland	**Symantec Asia Pacific Pte Ltd.** ☐ 6 Temasek Boulevard, #12-01 Suntec Tower 4, Singapore 038986
Signature:		
Printed Name and Title: LORRAINE WILLIAMS, PROCESS LEAD		
Date Signed: 07/03/2018		

Lorraine Williams
Symantec Limited

Exhibit 1

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

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

Other information needed to identify the organisation:

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

And

Name of the data importing organisation: .....

Address: .....

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

Other information needed to identify the organisation:

.....
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

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

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

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[1]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
As specified in the Addendum.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
As specified in the Addendum

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
As specified in the Addendum

Categories of data
The personal data transferred concern the following categories of data (please specify):
As specified in the Addendum

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
As specified in the Adendum

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
Provision of the Services.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

As specified in Exhibit 2 of the Addendum.

Exhibit 2

Technical and organizational measures

Symantec has taken and will maintain the appropriate administrative, technical, physical and procedural security measures, consistent with international information practices, for protection of the security, confidentiality and integrity of the personal data as described on Symantec's Customer Trust portal, accessible on http://www.symantec.com/connect/groups/customer-trust-group, or otherwise made reasonably available by Symantec.

* * *