HPE Partner Ready Partner Data Privacy and Data Protection Addendum

1. Introduction

To comply with data privacy and data protection laws and regulations, HPE must ensure data privacy and data protection provisions are incorporated into contracts between HPE, HPE Partner Ready partners and the Customer including documenting safeguards to protect exchanges of Personal Data controlled or processed by HPE, HPE Partner Ready partner and/or Customers.

This addendum to the HPE Partner Code of Conduct is incorporated into the HPE Partner Ready Partner Agreement (the “Agreement”) (“Addendum”) and sets out the obligations of HPE and HPE Partner Ready partner groups in relation to Personal Data controlled or processed by HPE, HPE Partner Ready partners, and/or Customer. Capitalized terms not specifically defined herein shall have the meaning set forth in the Agreement.

2. Definitions

“Approved Subcontractor” means any affiliate or third party contractor of Processor approved or deemed approved in accordance with section 3.26 or listed in the Agreement.

“Applicable Laws” means applicable local, state, and federal laws, including but not limited to the General Data Protection Regulation, executive orders, rules, regulations, ordinances, codes, orders, and decrees of all governments or agencies of domestic or foreign jurisdictions (including Privacy Laws) in which the Services are performed or to which the Services are performed pursuant to the Agreement.

“Approved Third Country” means any EEA country or any third country which is approved by the European Commission from time to time as providing adequate protection for personal data pursuant to Article 45(3) of the General Data Protection Regulation.

“Appointee” means HPE or the HPE Partner Ready partner that appoints the other as a Data Processor under section 3.1.

“Controller” means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data; where the purposes and means of Processing are determined by applicable Privacy Law, the Controller or the criteria for the Controller's nomination will be as designated by applicable Privacy Law.


“Data Processor” means any natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of a Controller or on the instruction of another Processor acting on behalf of a Controller.

“Data Subject” means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

“EEA Personal Data” means Personal Data which originates from a member state of the EEA, the UK or Switzerland.

“EU-US Privacy Shield Certification” means certification under the Privacy Shield framework administered by the US Department of Commerce.

“Personal Data” means any information relating to an identified or identifiable Data Subject (or as otherwise defined by Privacy Law), including Sensitive Personal Data.

“Privacy Law” means all applicable laws and regulations relating to the processing of Personal Data and privacy that may exist in the relevant jurisdictions.

“Privacy Authority” means the relevant supervisory authority with responsibility for privacy or data protection matters in a jurisdiction.

“Process”, “Processing”, or “Processed” means any operation or set of operations which is performed on or with Personal Data whether or not by automatic means (including, without limitation, accessing, collecting, recording, organizing, retaining, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Personal Data) and any equivalent definitions in Privacy Law to the extent that such definitions should exceed this definition.

“Processor” is as defined in section 3.

“Security Incident” means a security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to Personal Data.

“Sensitive Personal Data” means any information relating to a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, biometric and geolocation data or as otherwise defined by Privacy Law.

“Services” means the services provided by HPE or the HPE Partner Ready partner to the other under the Agreement.

3. Data Processing Obligations

HPE may be a Data Processor of an HPE Partner Ready partner where the HPE Partner Ready partner contracts with a Customer for any HPE Partner Ready partner branded services that include Products or Services provided by HPE to the HPE Partner Ready partner.

An HPE Partner Ready partner may be a Data Processor of HPE where HPE contracts with a Customer for HPE branded services that include Products or Services provided by the HPE Partner Ready partner to HPE.

The following terms shall apply where HPE or an HPE Partner Ready partner provides Products and/or Services to the other (or its Customers) and in doing so Processes Personal Data on behalf of the other (the “Appointee”) as a Data Processor (“Processor”) of which Appointee, its Affiliates, or Customers is the Controller and which Appointee, its Affiliates or Customers may provide or otherwise make available to Processor for Processing on its or their behalf in connection with the Products or Services.

3.1 To the extent HPE or an HPE Partner Ready partner processes Personal Data on behalf of the other under the Agreement, such party is hereby appointed by Appointee as a Data Processor in respect of all Personal Data Processed by it in order to provide the Products or Services. Processor shall Process the types and categories of Personal Data as set forth in Appendix 1 to the Controller to Processor EU Model Contract as required to execute this Agreement unless the Appointee agrees otherwise in subsequent documented instructions or statement of work.

3.2 Processor shall only Process Personal Data to the extent and in a manner necessary to provide the Services or the Products to the Appointee (or its Customers) and in accordance with documented instruction of Appointee (which may be specific or general in nature as set out in this Agreement or otherwise notified to Processor under the Agreement) and shall not Process Personal Data for any other purpose. Processor shall take appropriate steps to ensure that persons acting under its authority only Process Personal Data in accordance with these instructions.

3.3 Processor shall promptly notify Appointee in writing, unless prohibited from doing so under Applicable Law, if:

3.3.1 it believes that any instruction from Appointee violates Privacy Law (without having to conduct a comprehensive legal analysis);

3.3.2 it is unable to comply with Appointee’s instructions for any reason; or
3.3.3 it is unable to comply with Appointee’s instructions or the terms of the Agreement in relation to the Processing of Personal Data due to legislation applicable to it or arising as a result of a change to that legislation or the introduction of new legislation.

3.4 Processor acknowledges that it has no right, title or interest in Personal Data (including all intellectual property or proprietary information) and may not sell, rent or lease Personal Data to anyone.

3.5 Processor shall at all times comply with its obligations under applicable Privacy Law to which it is subject as a service provider and Data Processor of Personal Data for the Appointee or which is otherwise applicable to its information security, privacy and data protection obligations in connection with the Services or the Products.

3.6 Processor shall not knowingly perform its obligations under this Agreement in such a way as to cause Appointee, its Affiliates or Customers to be in breach of any requirement under applicable Privacy Law.

3.7 Processor shall co-operate with and provide Appointee with the assistance it deems necessary to ensure Personal Data is processed in compliance with Privacy Law applicable to Appointee, its Affiliates and Customers, including as specified in sections 3.10 and 3.17.

3.8 Any request for co-operation or assistance by Appointee pursuant to section 3.7 shall be made in writing setting out Appointee’s requirements and related instructions and shall be met by Processor to the extent reasonably possible and within a reasonable period of time. To the extent that compliance with this section 3.8, constitutes a change to the scope of the Services, the parties shall, acting reasonably, agree on appropriate amendments to the Agreement and the payment of any reasonable and material associated costs to Processor.

3.9 Processor shall implement appropriate physical, technical and organizational measures to ensure that Personal Data is protected against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access in particular where the processing involves transmission of data over a network, and against all other unlawful forms of processing. The technical and organizational measures shall ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature and scope, context and purpose of processing and risks of varying likelihood and severity for the rights and freedoms of individuals. These measures shall include, as appropriate, (a) pseudonymisation and encryption of personal data, (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.10 Processor shall provide reasonable assistance to Appointee, as required, to ensure that Appointee can comply with its obligations in relation to security, data breach notification, conducting privacy impact assessments and possible consultations with Privacy Authorities under Privacy Law, taking into account the nature of the processing and the information available to Processor.

3.11 Processor shall ensure that persons within its organization are authorized to access and Process Personal Data are subject to a statutory or contractual confidentiality obligation in respect of the Personal Data.

3.12 In the event that Processor experiences or reasonably suspects a Security Incident affecting Personal Data it shall without undue delay notify Appointee of the Security Incident. Processor will provide Appointee with updates on the status of the Security Incident until the matter has been remediated. The reports will include, without limitation, a description of the Security Incident, actions taken and remediation plans.

3.13 Proportionate to acts or omissions of Processor resulting in a Security Incident, Processor agrees to pay reasonable costs for: (i) legally required notice to individuals affected by the Security Incident; (ii) credit monitoring service for twelve months, except to the extent applicable law specifies a longer period for such credit monitoring services, in which case such longer period shall then apply.

3.14 Processor shall at the request and cost of Appointee:

3.14.1 provide reasonable assistance to Appointee in notifying a Security Incident to the Privacy Authority competent under the Privacy laws applicable to Appointee; and
3.14.2 provide reasonable assistance to Appointee in communicating a Security Incident to Data Subjects in cases where the data breach is likely to result in a high risk to the rights and freedoms of individuals.

3.15 Processor shall within 5 business days of receipt, forward to Appointee any request, complaint, notice or other communication from a Data Subject or a Privacy Authority in connection with Personal Data ("Communication") and will not respond to a Communication unless agreed with Appointee. Processor shall co-operate fully with Appointee in connection with a Communication and promptly provide Appointee with any information it reasonably requires to respond to the Communication. To the extent Appointee is not able to access Personal Data Processed by Processor itself, Processor shall promptly provide Appointee with any Personal Data in its possession in the form reasonably requested by Appointee as Appointee may reasonably require, including to respond to a Communication.

3.16 Taking into account the nature of the Processing, Processor shall assist Appointee with appropriate technical and organizational measures to fulfill Appointee and its Affiliates or its Customers’ obligations under Privacy Law to respond to requests from Data Subjects for exercising their rights of information, access, restriction, erasure, portability and objection in connection with Personal Data Processed by Processor.

3.17 To the extent that Appointee is not able to access Personal Data itself, Processor shall on Appointee’s written request (i) update, correct or delete Personal Data; and/or (ii) provide copies of Personal Data to Appointee.

3.18 Processor shall process Personal Data for the duration of the Agreement unless otherwise agreed to with Appointee. Upon termination of the Agreement, Processor shall, at the election of Appointee, return or delete Personal Data and Processor shall not retain copies of Personal Data unless otherwise agreed with Appointee or where it is required to do so under applicable law, in which case Appointee shall stop actively processing the data and maintain the security and confidentiality of the data.

3.19 If and to the extent Processor or its Affiliates Process EEA Personal Data in a country which is not an Approved Third Country and in order to ensure Appointee’s Processing of EEA Personal Data is in compliance with Appointee’s binding corporate rules, EU Model Contracts executed with Customers or applicable Privacy Law, the Controller to Processor EU Model Contract is hereby incorporated into this Agreement and Processor shall and shall ensure that its Affiliates comply with the obligations of a Data Importer (as defined in the Controller to Processor EU Model Contract) in its or their capacity as a Data Processor or sub-processor of Appointee or an Appointee’s Affiliate. To the extent there is any conflict between the terms of this Agreement and the Controller to Processor EU Model Contract, the terms of the Controller to Processor EU Model Contract shall prevail.

3.20 Processor acknowledges that Appointee or its Affiliates may act as (i) a Controller or (ii) as a Processor for a Customer in relation to the transferred EEA Personal Data and that this shall not prejudice the application of the EU Model Contract terms to the transfer and processing of that Personal Data by the Appointee or its Affiliates as a Data Importer in its capacity as a Data Processor or sub-processor of Appointee or its Affiliates. When interpreting the EU Model Contract in the term "Member State in which the data exporter is established" will be interpreted to mean (as appropriate) Switzerland or the EU or EEA member state in which the Data Exporter (as defined in the Controller to Processor EU Model Contract) is established. The parties agree that any losses suffered by either party or their Affiliates under a Controller to Processor EU Model Contract, shall be treated as if they had been suffered by HPE or the HPE Partner Ready partner respectively and shall in all cases be recovered by HPE or the HPE Partner Ready partner subject to any limits on that party’s liability in the Agreement. Nothing in this section 3.20 shall limit the liability of either party in relation to a claim by a Data Subject under the Controller to Processor EU Model Contract.

3.21 At Appointee’s request, Processor shall, or shall procure that the relevant Processor Affiliate:

3.21.1 executes the Controller to Processor EU Model Contract directly with Appointee or its Affiliates, where it deems it necessary in order to comply with binding corporate rules or applicable Privacy Law;

3.21.2 executes a form of onward transfer agreement based on the Controller to Processor EU Model Contract with Appointee or its Affiliates where it deems it necessary in order to comply with section 11 of a Controller to Processor EU Model Contract executed with a Customer by Appointee or its Affiliates.

3.22 Where HPE is the Appointee and if applicable, HPE agrees to rely on HPE Partner Ready partner’s EU-US Privacy Shield Certification to provide adequate protection for any EEA Personal Data which is
transferred to or accessed by a certified HPE Partner Ready partner or its certified U.S. Affiliates. The HPE Partner Ready partner warrants that it and or its Affiliates are and shall remain certified under the EU-US Privacy Shield Framework run by the US Department of Commerce. Processor shall promptly notify HPE if it does not renew its EU-US Privacy Shield Certification. In the event that the HPE Partner Ready partner or its Affiliates does not renew its EU-US Privacy Shield Certification or the EU-US Privacy Shield Framework is invalidated as a transfer mechanism, the Controller to Processor EU Model Contract and sections 3.19-3.21 shall apply to EEA Personal Data which is transferred to or accessed by Processor in the U.S. or its U.S. Affiliates.

3.23 Appointee or its Affiliates shall be responsible for any notifications or approvals required from a Privacy Authority in relation to their reliance on a Controller to Processor EU Model Contract and/or an EU-US Privacy Shield Certification. Processor shall provide Appointee or its Affiliates with all reasonable assistance in relation to any such regulatory approvals or notifications.

3.24 Appointee or its Affiliates are permitted to disclose to a Privacy Authority this Addendum and any other privacy and security sections of the Agreement and any data transfer agreement, as necessary in connection with a regulatory notification or approval.

3.25 Processor may only disclose (including permit access to) Personal Data to an Affiliate or third-party subcontractor after having (i) notified Appointee and obtained its specific or general written authorization of Appointee and (ii) complied with section 3.27, unless such disclosures are required under Applicable Law. In this case, Processor will inform Appointee in advance of these disclosures, unless prohibited from doing so under Applicable Law, and work with Appointee to ensure that the disclosures occur in compliance with Privacy Law. The subprocessors applicable to HPE services and locations of processing can be found at www.hpe.com/info/customer-privacy.html and are deemed as approved by the HPE Partner Ready partner. HPE Partner Ready partner will subscribe to HPE’s notification tool on the above website, and in the event of changes to approved subprocessors, HPE will notify the HPE Partner Ready partner via the notice subscription tool.

3.26 Appointee shall have ten 10 business days from receipt of a notice of disclosure pursuant to Section 3.25 to make an assessment of the disclosure. If Appointee does not object to the disclosure within this time period it shall be deemed to have consented and the affiliate or third-party subcontractor shall qualify as an Approved Subcontractor. If Appointee reasonably objects to the disclosure, Processor shall make disclosures of Personal Data to a Processor’s affiliate or third-party subcontractor and the parties commit to cooperate to come to a mutually acceptable solution.

3.27 Processor may only disclose Personal Data to an Approved Subcontractor after:

3.27.1 Appointee has been provided with details of each country in which Personal Data is proposed to be Processed by the Approved Subcontractor;

3.27.2 it has executed a valid and enforceable written contract with the subcontractor (which may include an inter-company agreement in the case of Processor Affiliates) containing privacy and security provisions substantially similar to those contained in this Addendum;

3.27.3 it has put in place appropriate measures to ensure that international transfers of Personal data occur in compliance with Privacy Law.

3.28 Processor shall be responsible for the acts and omissions of Approved Subcontractors it engages to provide the Services to Appointee and remains fully liable for the acts and omissions of the Approved Subcontractors giving rise to a breach of this Agreement as if they were its own acts or omissions.

3.29 Processor shall make available to Appointee all information necessary to demonstrate compliance with Section 3. Appointee can audit Processor’s compliance with this Addendum in accordance with the audit provisions in the Agreement.

4. Disclosures of Personal Data

4.1. Processor and Appointee shall each disclose to the other contact information relating to their respective representatives (including via usage of the HPE Partner Ready Portal) (“Business Contact Data”) which shall be used for (i) invoicing, billing and other business inquiries, (ii) information on usage of the Services,
(iii) contract management. HPE shall also use Business Contact Data to send email communications to Partner’s representatives. These communications are limited to:

4.1.1 messages of an operational and administrative nature related to the HPE channel space, or messages about the status and use of the HPE Partner Portal;
4.1.2 regular (weekly or monthly) business awareness communications (newsletters) which are relevant to HPE partners;
4.1.3 occasional communications related to specific HPE sales and marketing operations or campaigns that may benefit partner’s customer;
4.1.4 certification and learning communications which impact a representative’s partner status on the HPE Partner Ready program; or
4.1.5 invitations to respond to surveys on the HPE Partner Ready Program.

Each party shall comply with all applicable laws and their respective privacy policies with respect to the Processing of Business Contact Data and use Business Contact Data only for the purposes outlined in section 4.1.

4.2. Where compliant with applicable law, HPE and the HPE Partner Ready partner may disclose to one another Personal Data relating to their respective Customers for use by the recipient party for the purposes of:

4.2.1.1 sending Product or Service related communications to Customers;
4.2.1.2 registering Customers for support in relation to Services or Products;
4.2.1.3 contacting a Customer about contract renewals;
4.2.1.4 confirming whether marketing activities conducted by or on behalf of the other have resulted in lead generation for sales purposes and related lead generation management activities;
4.2.1.5 proving execution of HPE Partner Ready program requirements or compliance with activities for HPE benefit payments; or
4.2.1.6 follow up contact with Customers identified by HPE or the HPE Partner Ready partner as sales opportunities (the “purposes”).

4.3 The parties acknowledge and agree that they shall each Process such Personal Data as Controllers and shall at all times comply with their respective obligations under applicable Privacy Law and in accordance with their privacy policies.

4.4 Notwithstanding HPE Partner Ready partner’s role as Controller in this context, HPE Partner Ready partner is prohibited from retaining, using, disclosing (including but not limited to in exchange for monetary or other valuable consideration) Personal Data for purposes other than the Purposes, unless and until it has ascertained that the Processing for another purpose is based on a proper lawful basis and the parties agree to any such additional purpose(s) in writing. HPE Partner Ready partner certifies that it understands the restrictions in this section 4.4 and that it will comply with them.

4.5 If and to the extent disclosure of Personal Data by one party to the other for the Purposes requires the transfer of Personal Data to a country which is not an Approved Third Country, the Controller to Controller EU Model Contract is hereby incorporated into this Agreement and each party shall and shall ensure that their respective Affiliates comply (as applicable) with the obligations of a Data Exporter or Data Importer (as defined in the Controller to Controller EU Model Contract). To the extent there is any conflict between the terms of this Agreement and the Controller to Controller EU Model Contract, the terms of the Controller to Processor EU Model Contract shall prevail. When interpreting the Controller to Controller EU Model Contract the term “Member State in which the data exporter is established” will be interpreted to mean (as appropriate) Switzerland or EEA member state in which the Data Exporter is established. The parties agree that any losses suffered by either party or their Affiliates under a Controller to Controller EU Model Contract, shall be treated as if they had been suffered by HPE or the HPE Partner Ready partner respectively and shall in all cases be recovered by HPE or the HPE Partner Ready partner subject to any limits on that party’s liability in the Agreement. Nothing in this section 4.5 shall limit the liability of either party in relation to a claim by a Data Subject under the Controller to Controller EU Model Contract.

4.6 At HPE or an HPE Partner Ready partner’s request, both parties shall, or shall procure that their relevant Affiliates execute the Controller to Controller EU Model Contract, where it is deemed necessary by either party to comply with binding corporate rules or applicable Privacy Law.
4.7 In the case of transfers from HPE or its Affiliates to an HPE Partner Ready partner or its Affiliates, if applicable, HPE agrees to rely on HPE Partner Ready partner’s EU-US Privacy Shield Certification to provide adequate protection for any EEA Personal Data which is transferred to or accessed by a certified HPE Partner Ready partner or its certified U.S. Affiliates. The HPE Partner Ready partner warrants that it and/or its Affiliates are and shall remain certified under the EU-US Privacy Shield Framework run by the US Department of Commerce. The HPE Partner Ready partner shall promptly notify HPE if it does not renew its EU-US Privacy Shield Certification. In the event that the HPE Partner Ready partner or its Affiliates does not renew its EU-US Privacy Shield Certification or the EU-US Privacy Shield Framework is invalidated as a transfer mechanism, the Controller to Controller EU Model Contract and sections 4.5 – 4.7 shall apply to EEA Personal Data which is transferred to or accessed by the HPE Partner Ready partner in the U.S. or its U.S. Affiliates.
Annex 1
EU Controller to Processor Model Contract

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,

Data Exporter and Data Importer (as defined in Appendix 1), 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 sub-processor” means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with 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 sub-processor 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 sub-processor 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 sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of 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 sub-processor 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 sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

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

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 sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-
processor shall be limited to its own processing operations under the Clauses.

**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 sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to 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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in 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 sub-processor 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 sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

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

Data Exporter:  
Authorized Representative  
Date  
Printed name  
Title

Data Importer:  
Authorized Representative  
Date  
Printed name  
Title
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):

Appointee and/or its affiliated companies.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Processor and/or its affiliated companies located outside the EEA or Switzerland

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Personnel, business contacts, Customers of the data exporter, or its Customers (where applicable).

Categories of data

The personal data transferred concern the following categories of data (please specify):

Name, contact information and any other personal data processed by the data importer in order to provide the Products or Services acquired by the data exporter.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

The following special categories of data may be processed by the data importer where permitted by the data exporter and as required to provide the Products or Services acquired by the data exporter:

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health, sex life or sexual orientation.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The personal data will be processed by the data importer as required to provide the Products or Services acquired by the data exporter from the data importer.

Data Exporter: [Signature] Data Importer: [Signature]
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):

The data importer shall implement the physical, technical and organisational security measures specified section 3.9 of the Addendum.

Data Exporter: [Signature]  
Data Importer: [Signature]

Date  
Date

Printed name  
Printed name

Title  
Title
Annex 2

Controller to Controller EU Model Contract

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

Between

...........................................................................................................................................(name)

..........................................................................................................................................(address and country of establishment)

hereinafter “data exporter”

and

...........................................................................................................................................(name)

..........................................................................................................................................(address and country of establishment)

hereinafter “data importer”

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

b) “the data exporter” shall mean the controller who transfers the personal data;

c) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.
I. Obligations of the data exporter

The data exporter warrants and undertakes that:

   a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

   b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

   c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

   d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

   e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

   a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

   b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

   c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

   d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

   e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).
f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

iii. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: A

Initials of data importer: ............................................................

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageuous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party

---

1 “Relevant provisions” means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

2 However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.
rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter’s country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter’s country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter’s country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or
v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

IX. Counterparts

The Clauses may be entered into in any number of counterparts, all of which taken together shall constitute one and the same instrument. This agreement to the extent signed and delivered by means of facsimile or as an attachment to an electronic mail message in “pdf” or similar format, shall be treated in all manner and respect as an original agreement or instrument and shall be considered to have the same binding legal effect as if it were the original signed version thereof delivered in person.

Data Exporter:          Data Importer:

Authorized Representative          Authorized Representative

Date          Date
<table>
<thead>
<tr>
<th>Printed name</th>
<th>Printed name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Title</td>
</tr>
</tbody>
</table>
ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   ii. the data subject is given an opportunity to discuss the results of a relevant automated
decision with a representative of the parties making such decision or otherwise to make representations to that party.

or

b) where otherwise provided by the law of the data exporter.
ANNEX B

DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

Data subjects
The personal data transferred concern the following categories of data subjects:

Customers of the data exporter.

Purposes of the transfer(s)
The transfer is made for the following purposes:

To enable the data importer to:

(i) send Product or Service related communications to Customers;
(ii) register Customers for support in relation to Services or Products;
(iii) contact Customer about contract renewals;
(iv) confirm whether marketing activities conducted by or on behalf of the other have resulted in lead generation for sales purposes and related lead generation management activities;
(v) prove execution of HPE Partner Ready program requirements or compliance with activities for HPE benefit payments; or
(vi) follow up contact with Customers identified by HPE or the HPE Partner Ready partner as sales opportunities.

Categories of data
The personal data transferred concern the following categories of data:

Name and business contact details.

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients:

Affiliated entities of the data importer, its service providers and professional advisors.

Sensitive data (if appropriate)
The personal data transferred concern the following categories of sensitive data:

None

Contact points for data protection enquiries

<table>
<thead>
<tr>
<th>DATA IMPORTER</th>
<th>DATA EXPORTER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>