This Data Processing Addendum ("DPA") and applicable Attachments apply to Personal Data by HP and/or Partner (the "Parties") that is processed in connection with the Services provided under the HP Partner Agreement, HP Business Partner Terms or any similar agreement or terms between HP and a partner (collectively known as “Partner Agreement”). This DPA does not apply where HP acts as a Data Processor directly to the Customer and is instructed by the Customer to share Personal Data with Partner. Capitalized terms not specifically defined herein shall have the meaning set out in the applicable Partner Agreement. In the event of a conflict between the terms of the Partner Agreement as it relates to the processing of Personal Data and this DPA, the DPA shall prevail.

1 DEFINITIONS

1.1 "Customer" means the customer of HP Services;

1.2 "Data 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 Data Protection and Privacy Laws, the Data Controller or the criteria for the Data Controller’s nomination will be as designated by applicable Data Protection and Privacy Laws;

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

1.4 "Data Protection and Privacy Laws" means all current and future applicable laws and regulations relating to the processing, security, protection, and retention of Personal Data and privacy that may exist in the relevant jurisdictions, including, but not limited to, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, any national laws or regulations implementing the foregoing Directives, the GDPR (when applicable), and any data protection laws of Norway, Iceland, Liechtenstein, Switzerland or the UK and any amendments to or replacements for such laws and regulations;

1.5 "Data Subject" shall have the meaning assigned to the term “data subject” under applicable Data Protection and Privacy Laws and shall include, at the minimum, any and all identified or identifiable natural person to whom the Personal Data relates;

1.6 "EU" means the European Union and the countries which are members of that union collectively;

1.7 "European Country" means a member state of the EU, Norway, Iceland, Liechtenstein, Switzerland and the UK;

1.8 "EU Standard Contractual Clauses (controllers)" means the EU standard contractual clauses for the transfer of Personal Data from Data Controllers to Data Controllers foreseen in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 or it successor;

1.9 "EU Standard Contractual Clauses (processors)" means the EU standard contractual clauses for the transfer of Personal Data from Data Controllers to Data Processors foreseen in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 or it successor;
1.10 “EU Standard Contractual Clauses (sub-processors)” means the EU standard contractual clauses for the transfer of Personal Data from Data Processors to Data Processors foreseen in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 or its successor;

1.11 “GDPR” means the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;


1.13 “Personal Data” means any information relating to an identified or identifiable living individual or as otherwise defined by applicable Data Protection and Privacy Laws. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity. For purposes of this DPA, Personal Data may include data in which (i) either Party is the Data Controller and which is processed by the other Party in the course of providing the Services under the Partner Agreement and/or; 2) a Customer is the Data Controller and which is processed by either Party as a sub-processor to the other Party in the course of providing the Services under the Partner Agreement. Personal Data also includes Protected Health Information, which is specifically addressed in Section 3 of this DPA;

1.14 “Personal Data Incident” shall have the meaning assigned by applicable Data Protection and Privacy Laws to the terms “security incident”, “security breach” or “personal data breach” but shall include any situation in which HP and/or Partner becomes aware that Personal Data has been or is likely to have been accessed, disclosed, altered, lost, destroyed or used by unauthorized persons, in an unauthorized manner;

1.15 “Privacy Authority” means the relevant public authority with jurisdiction over privacy or data protection matters;

1.16 “process”, “processes”, “processing” or “processed” means any operation or set of operations which is performed upon Personal Data whether or not by automatic means, including, without limitation, accessing, collecting, recording, organizing, structuring, retaining, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning, combining, blocking, restricting, erasing and destroying Personal Data and any equivalent definitions in applicable Data Protection and Privacy Laws to the extent that such definitions should exceed this definition;

1.17 “Protected Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information” in HIPAA (45 CFR 160.103) and shall refer to PHI held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral;

1.18 “Relevant Country” means all countries other than those European Countries and other countries in respect of which there is an adequacy finding under Article 25(6) of the European Data Protection Directive or Article 45 of the GDPR;

1.19 “Services” means services, including products and support, provided by HP and/or Partner under the Partner Agreement;

1.20 “Sub-processor” means any natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of a Data Processor acting on behalf of a Data Controller;

2 PROCESSING OF PERSONAL DATA

2.1 Scope & Compliance with Law

September 2021
2.1.1 The categories of Data Subjects, types of Personal Data and purposes of processing are set out in Attachment 1 of this DPA. Personal Data shall be processed for the duration of the Partner Agreement (or longer to the extent required by applicable law).

2.1.2 Each Party shall:

2.1.2.1 be responsible for compliance with all applicable Data Protection and Privacy Laws regarding the accuracy, quality and legality of Personal Data that is to be transferred to and processed by the other Party in connection with the Services provided under the Partner Agreement;

2.1.2.2 ensure that the instructions it provides to the other Party in relation to the processing of Personal Data shall comply with all applicable Data Protection and Privacy Laws and shall not put the other Party in breach of its obligations under applicable Data Protection and Privacy Laws; and

2.1.2.3 act at its own risk and assume responsibility of any compliance deficits related to the processing of Personal Data not expressly covered by the scope of this DPA or the Partner Agreement.

2.1.3 Where the Parties disclose any Personal Data of their employees or where such Personal Data is provided directly by the employee to the Parties, the Parties shall process that Personal Data in accordance with their privacy policies and applicable Data Protection and Privacy Laws. Such disclosures shall be made by the Parties only where lawful for the purposes of contract management, service management or for the purposes of reasonable background screening verification or security.

2.2 Data Processor Obligations

2.2.1 Notwithstanding anything to the contrary in the Partner Agreement, each Party, to the extent that it is acting as a Data Processor to the other Party, shall:

2.2.1.1 only process Personal Data in accordance with documented instructions (which may be specific or general in nature as set out in the Partner Agreement or as otherwise notified by the Parties). Notwithstanding the foregoing, the Parties may process Personal Data as required under applicable law. In this situation, each Party shall take reasonable steps to inform the other Party of such a requirement before it processes the data, unless the law prohibits this;

2.2.1.2 ensure only authorized personnel who have undergone the appropriate training in the protection and handling of Personal Data and are bound to respect the confidentiality of Personal Data shall have access to the same;

2.2.1.3 implement appropriate technical and organizational measures to protect against unauthorized or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of Personal Data and having regard to the nature of the Personal Data;

2.2.1.4 without undue delay and to the extent permitted by law, notify the other Party of any requests from Data Subjects seeking to exercise their rights under applicable Data Protection and Privacy Laws and, at the other Party’s written request and cost, taking into account the nature of the processing, assist the other Party by implementing appropriate technical and organizational measures, insofar as this is possible, to assist with the other Party’s obligation to respond to such requests. To the extent that
Personal Data is not accessible to the other Party through the Services provided under the Partner Agreement, each Party shall, where legally permitted and upon request by the other, provide commercially reasonable efforts to assist the other Party in responding to such requests if responses to such requests are required by the applicable Data Protection and Privacy Laws;

2.2.1.5 upon written request by the other Party and taking into account the nature of processing and the information available, provide reasonable assistance to the other Party in connection with obligations under Articles 32 to 36 of the GDPR or equivalent provisions under applicable Data Protection and Privacy Laws; and

2.2.1.6 upon written request, delete or return any such Personal Data after the end of the provision of the Services, unless applicable law requires storage of the Personal Data.

2.3 Sub-Processing

2.3.1 Each Party, to the extent that it is acting as a Data Processor to the other Party, is authorized to appoint affiliated and third-party Sub-processors (and permit each Sub-processor to appoint in accordance with Clause 2.3.1) for the provision of Services under the Partner Agreement. The Parties shall remain responsible for its Sub-processor’s compliance with the obligations of this DPA. The Parties shall ensure that any Sub-processors to whom Personal Data is transferred enter into written agreements requiring that the Sub-processors abide by terms no less protective than those set forth in this DPA.

2.3.2 The Parties may continue to use those Sub-processors already engaged as of the date of this DPA.

2.3.3 Each Party, to the extent that it is acting as a Data Processor to the other Party can at any time and without justification appoint a new Sub-processor provided that the other Party is given ten (10) days’ prior notice and the other Party does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Sub-processor’s non-compliance with applicable Data Protection and Privacy Laws. If, in the notifying Party’s reasonable opinion, such objections are legitimate, the notifying Party shall refrain from using such Sub-processor in the context of the processing of Personal Data. In such cases, the notifying Party shall use reasonable efforts to (i) make available a change in the Services or (ii) recommend a change to the configuration or use of the Services to avoid the processing of Personal Data by the objected-to Sub-processor. If the notifying Party is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, the objecting Party may, by providing written notice, terminate the Service which cannot be provided by the notifying Party without the use of the objected-to Sub-processor by providing written notice.

2.4 Personal Data Incidents

2.4.1 Each Party, without undue delay, shall notify the other if it becomes aware of any Personal Data Incident and take such steps as reasonably required to remedy the Personal Data Incident, to assist in any investigation and to provide sufficient information to meet any obligations to report the Personal Data Incident to the appropriate Privacy Authority and/or Data Subjects.

2.5 International Transfers of Partner Personal Data

2.5.1 The Parties may transfer Personal Data outside the country from which it was originally collected provided that such transfer is required in connection with the provision of Services under the Partner Agreement and such transfers take place in accordance with applicable Data Protection and Privacy Laws.
2.5.2 European Specific Provisions

2.5.2.1 To the extent that Personal Data is transferred to a Relevant Country the EU Standard Contractual Clauses (processors) (Attachment 2) apply to any transfers of Personal Data from a European Country to a Relevant Country in accordance with applicable Data Protection and Privacy Laws. The EU Standard Contractual Clauses (sub-processors) (Attachment 3) apply, instead of the EU Standard Contractual Clauses (processors), in cases where the Party in the European Country act as a Data Processor and the Party in the Relevant Country acts as a Sub-processor. The EU Standard Contractual Clauses (processors) are hereby incorporated in their entirety into this DPA and, to the extent applicable, the Parties shall ensure that their Sub-processors comply with the obligations of a data importer (as defined in the EU Standard Contractual Clauses). To the extent there is any conflict between this DPA and the EU Standard Contractual Clauses Contract, the terms of the EU Standard Contractual Clauses shall prevail.

2.5.2.2 To the extent that the Parties act as Data Controllers in their own right, any transfers of Personal Data from a European Country to a Relevant Country, must take place in accordance with the EU Standard Contractual Clauses (controllers) (Attachment 4) which is hereby incorporated in its entirety into this DPA.

2.6 Audits

2.6.1 Upon written request, each Party shall make available to the other all information necessary to demonstrate compliance with the obligations set forth under applicable Data Protection and Privacy Laws, provided that the Parties shall have no obligation to provide commercially confidential information. On no more than an annual basis and at the requesting Party’s expense, the Parties shall further allow for and contribute to audits and inspections by the other or its authorized third-party auditor that not shall be a competitor of the audited Party. The scope of any such audits, including conditions of confidentiality, shall be mutually agreed upon by the Parties prior to initiation.

2.7 Liability

2.7.1 Liability arising out of or related to processing of Personal Data in accordance with this DPA (whether in contract, tort or under any other theory of liability) is subject to any limitations of liability provision(s) as set forth in the Partner Agreement.

3 HANDLING OF U.S. PROTECTED HEALTH INFORMATION BY PARTNER

3.1 Scope & Compliance with Law

3.1.1 This section of the DPA shall only apply to Partners doing business in the U.S. and those outside of the U.S. that are acting as a Business Associate, as defined by HIPAA.

3.1.2 HIPAA applies to the following two categories of individuals, organizations and agencies:

3.1.2.1 Covered Entity – shall have the same meaning as the term “Covered Entity” in 45 CFR 160.103 and refers to health care providers (e.g., doctors, hospitals, medical facilities, dentists, pharmacies), health plans (e.g., health insurance companies, company health plans, and government programs that pay for healthcare) and healthcare clearinghouses, as those entities are defined in 45 CFR 160.103; and

3.1.2.2 Business Associate – shall have the same meaning as the term “Business Associate” in 45 CFR 160.103 and, as used in this DPA, refers to an entity that creates, maintains,
receives, or transmits PHI while providing Services to a Covered Entity and/or a Business Associate.

3.1.3 Partner, when acting as a Business Associate, shall safeguard PHI that Partner creates, receives, maintains, or transmits on behalf of a Covered Entity or Business Associate in accordance with the requirements of HIPAA, as amended from time to time.

3.1.4 HIPAA requires that relationships between a Covered Entity and Business Associate must be governed by a Business Associate Agreement (“BAA”). In addition, where a Business Associate uses sub-contractors or partners in providing those Services, the obligations of the BAA must flow down to the sub-contractors or partners. At HP, this flow-down BAA is called an Agent/Subcontractor Agreement (“ASA”).

3.2 Obligations of HP Partner

3.2.1 Partners must understand the legal requirements when HP and Partners are providing Services to Customers who are either Covered Entities or Business Associates, as well as HP’s implementation of HIPAA as applied to its channel partner program.

3.2.2 Where HP or Partners sell Services to either Covered Entities or Business Associates and there is access or potential access to PHI during delivery of the Services, the Partner shall, where applicable:

3.2.2.1 ensure that HP’s pass-through BAA is executed with the Customer as part of the overall HP terms that attach to the affected Services;

3.2.2.2 execute with HP an ASA that flows down the requirements included in HP’s pass-through BAA with the Customer (either Covered Entity or Business Associate); and

3.2.2.3 ensure that the appropriate ASAs have been executed with Partner’s sub-contractors.
Details of Processing

HP may periodically update this Attachment 1 to reflect changes in processing activities.

Categories of Data Subjects

Personal Data that may be processed by HP and/or Partner in connection with the provision of the Services under the Partner Agreement may include relates to the following data subjects:

- Customers
- Customers’ employees, agents and subcontractors
- HP & Partner employees

Types of Personal Data

The types of Personal Data that may be processed by HP and/or Partner in connection with the provision of the Services under the Partner Agreement may include:

- Contact data - such as name, phone number, email address and office address;
- Security credentials data - such as passcodes, employee identification or badge number;
- Product usage data – such as pages printed, print mode, media used, ink or toner brand, file type printed (.pdf, .jpg, etc.), application used for printing (Word, Excel, Adobe Photoshop, etc.), file size, time stamp, and usage and status of other printer supplies;
- Performance Data – Printing events, features, and alerts used such as “Low on Ink” warnings, use of photo cards, fax, scan, embedded web server, and additional technical information that varies by product;
- Device Data – information about the computer, printer and/or device such as operating system, amount of memory, region, language, time zone, model number, first start date, age of device, device manufacture date, browser version, computer manufacturer, connection port, warranty status, unique device identifiers, advertising identifiers and additional technical information that varies by product;
- Application Data – information related to HP applications such as location, language, software versions, data sharing choices and update details;
- Personal certification and performance data; and
- Other Personal Data provided by Data Subject when she/he interacts in-person, online or by phone by the person, or mail with services centers, help desks or other customer support channels to facilitate delivery of HP Services and to respond to Customer and/or Data Subject inquiries.

Processing activities

Personal Data processed in connection with the Partner Agreement shall be used by HP and/or Partner to manage the relationship with and provide Services to the Customer. HP and/or Partner may process Customer Personal Data to:

- support sales activity including lead generation, tender pursuits, marketing and training;
- deliver fleet management services such as Managed Print Services and Device as a Service;
- maintain accurate contact and registration data to deliver comprehensive support and maintenance services, including care-pack and extended warranty support and facilitating repairs and returns;
- facilitate access to portals for ordering and completing orders for products or services, for the purposes of administering accounts and arranging shipments and deliveries;
• improve the performance and operation of products, solutions, services and support, including warranty support and timely firmware and software updates and alerts to ensure the continued operation of the device or service;

• provide administrative communications about the Services. Examples of administrative communications may include responses to inquiries or requests, service completion or warranty-related communications, safety recall notifications, or applicable corporate updates related to mergers, acquisitions or divestitures;

• maintain the integrity and security of HP’s websites, products, features and services and preventing and detecting security threats, fraud or other criminal or malicious activity that might compromise personal data;

• verify identities, including requesting the caller’s name and employee identification or badge number for the delivery of HP’s remote maintenance services;

• comply with applicable laws, regulations, court orders, government and law enforcement requests and to protect employees and other customers and to resolve disputes; and

• deliver a tailored experience, personalize the Services and communications and create recommendations.
Attachment 2

STANDARD CONTRACTUAL CLAUSES (UK processors)

These Standard Contractual Clauses (processors) are attached to and made part of the Data Protection Agreement (“DPA”) between HP and Customer.

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 are 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.

1 Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.
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 sub processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub processing, the processing activity is carried out in accordance with Clause 11 by a sub processor providing at least the same level of protection for the personal data and the rights of data 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

---

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.
by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of 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 sub processing, it has previously informed the data exporter and obtained its prior written consent;

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

(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 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 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
Sub-processing

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

---

3 This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.
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.
APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

These Standard Contractual Clauses (processors) are attached to and made part of the Data Protection Agreement (“DPA”) between HP and Customer. This Appendix forms part of the Clauses. 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):

The data exporter is the legal entity that has executed the Services Agreement and all affiliates of Customer established within a European Country that have purchased Services in accordance with the Services Agreement.

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

HP Inc. (1501 Page Mill Road, Palo Alto, CA 94304) together with all its majority owned and controlled subsidiaries irrespective of jurisdiction of incorporation or operation (“HP Group”) as providers of the Services set forth in the applicable Services Agreement.

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

See Attachment 1.

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

See Attachment 1.

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

See Attachment 1.

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

See Attachment 1.
APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

These Standard Contractual Clauses (processors) are attached to and made part of the Data Protection Agreement (“DPA”) between HP and Customer. This Appendix forms part of the Clauses.

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

Data importer will maintain administrative, physical and technical safeguards for protection, security and confidentiality of Personal Data processed in connection with the provision of Services provided under the applicable Services Agreement. The specific safeguards may vary depending on the nature of the Services provided under the Services Agreement.
Attachment 3 – Other Specified Transfer Mechanisms

STANDARD CONTRACT CLAUSES (Argentina)

In accordance with the provisions of clause 6.3.1 of the Data Processing Addendum, HP may, if required in connection with the services, transfer Customer Personal Data, originally collected in the Argentine Republic, to third countries.

If the transfer mentioned in the preceding paragraph implies transfer of Customer Personal Data to countries that are not considered as countries that provide adequate levels of protection by applicable Data Protection and Privacy Laws in Argentina, the EU Standard Contractual Clauses included in Attachment 2, with the modifications set forth below, shall be applicable to transfer.

1. Clause 1, items (a), (c) and (e) shall be replaced as follows:
   (a) ‘personal data’, ‘sensitive data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as set forth in the Argentine Data Protection Law No. 25,326, its regulatory Decree No. 1558/2001, and their complementary regulations (as amended or replaced from time to time);
   (c) “the data importer” means the service provider located outside of Argentina that receives the personal data from the data exporter for the processing in accordance with the terms of this agreement;
   (e) ‘the applicable data protection law’ means the Argentine Data Protection Law No. 25,326 and its supporting regulations (as amended or replaced from time to time).

2. Clause 4, item (f) shall be replaced as follows:
   (f) that 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 the Argentine Data Protection Law 25,326 and its supporting regulations (as amended or replaced from time to time).

3. Clause 7, subsection 1, item (b) shall be replaced as follows:
   (b) to refer the dispute to the judicial and administrative jurisdiction of the Argentine Republic.

4. Clause 9 shall be replaced as follows:

   This agreement shall be governed by the laws of the Argentine Republic, in particular by the Law No. 25,326, its regulations and dispositions issued by the Argentine Data Protection Authority (as amended or replaced from time to time),