CUSTOMER DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") and applicable Attachments apply when HP processes Customer Personal Data in order to provide the Services agreed to in the applicable agreement(s) between HP and Customer ("Services Agreement"). Capitalized terms not specifically defined herein shall have the meaning set out in the Services Agreement. In the event of a conflict between the terms of the Services Agreement as they relate to the processing of Personal Data and this DPA, the DPA shall prevail.

1 DEFINITIONS

1.1 **"Customer"** means the end-user customer of HP Services;

1.2 **"Customer Personal Data"** means the Personal Data in relation to which the Customer is the Data Controller and which is processed by HP as a Data Processor or its Sub-processors in the course of providing the Services;

1.3 **"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 Law, the Data Controller or the criteria for the Data Controller's nomination will be as designated by applicable Data Protection and Privacy Laws;

1.4 **"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;

1.5 **"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 the GDPR, 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, and any data protection laws of Norway, Iceland, Liechtenstein, Switzerland or the UK (once the UK has ceased to be part of the EU) and any amendments to or replacements for such laws and regulations;

1.6 **"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 persons to whom the Personal Data relates;

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

1.8 **"European Country"** means a member state of the EU, Norway, Iceland, Liechtenstein, Switzerland and the UK, once the UK has ceased to be a member state of the EU;

1.9 **"EU Standard Contractual Clauses"** means the EU standard contractual clauses for the transfer of Personal Data to Data Processors 2010/87/EU or its successor;

1.10 **"EU-U.S. Privacy Shield"** means the EU-U.S. Privacy Shield framework established by the U.S. Department of Commerce and the European Commission as amended or replaced from time to time;

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;

1.12 **"HP Group"** means HP Inc. (1501 Page Mill Road, Palo Alto, CA 94304) and all its majority owned and controlled subsidiaries irrespective of jurisdiction of incorporation or operation;

1.13 **"Personal Data"** means any information relating to an identified or identifiable 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;

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 becomes aware that Customer 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 **"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;

1.16 **"Processor Binding Corporate Rules"** mean binding corporate rules for Data Processor approved by certain Privacy Authorities in the EU;

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

1.18 **"Services"** means services, including products and support, provided by HP under the Services Agreement;

1.19 **"Services Agreement"** means the agreement between HP and Customer for the purchase of Services from HP; and

1.20 **"Sub-processor"** means any entity engaged by HP, where HP is acting as Processor, or by any other Sub-processor of HP who receives Customer Personal Data for processing activities to be carried out on behalf of Customer.

2 SCOPE & COMPLIANCE WITH LAW

2.1 This DPA applies to the processing of Customer Personal Data by HP in connection with HP's provision of the Services and when HP acts as a Data Processor on behalf of the Customer as the Data Controller. To the extent each Party is an independent Data Controller, it shall determine the purposes and means of its processing of Personal Data and shall comply with the obligations applicable to it under all applicable Data Protection and Privacy Laws. Nothing in this Section 2.1 shall modify any restrictions applicable to either Party's rights to use or otherwise process Personal Data under the Agreement between the Parties and the Parties shall process Personal Data solely and exclusively for the purposes specified in such Agreement.

2.2 The categories of Data Subjects, types of Customer Personal Data processed and purposes of processing are set out in Attachment 1 of this DPA. HP shall process Customer Personal Data for the duration of the Services Agreement (or longer to the extent required by applicable law).

2.3 Customer, in its use of HP's Services, shall have sole responsibility for compliance with all applicable Data Protection and Privacy Laws regarding the accuracy, quality and legality of Customer Personal Data that is to be processed by HP in connection with the Services. Customer shall further ensure that the instructions it provides to HP in relation to the processing of Customer Personal Data will comply with all applicable Data Protection and Privacy Laws and shall not put HP in breach of its obligations under applicable Data Protection and Privacy Laws.

2.4 If the Customer uses the Services to process any categories of Personal Data not expressly covered by this DPA, Customer acts at its own risk and HP shall not be responsible for any potential compliance deficits related to such use.

2.5 Where HP discloses any HP employee Personal Data to the Customer or an HP employee provides Personal Data directly to the Customer, which the Customer processes to manage its use of the Services, Customer shall process that Personal Data in accordance with its privacy policies and applicable Data Protection and Privacy Laws. Such disclosures shall be made by HP only where lawful for the purposes of contract management, service management or the Customer's reasonable background screening verification or security purposes.

3 OBLIGATIONS OF DATA PROCESSOR

3.1 Notwithstanding anything to the contrary in the Services Agreement, in relation to Customer Personal Data, HP shall:

3.1.1 only process Customer Personal Data in accordance with Customer's documented instructions (which may be specific or general in nature as set out in the Services Agreement or as otherwise notified by Customer). Notwithstanding the foregoing, HP may process Customer Personal Data as required under applicable law. In this situation, HP will take reasonable steps to inform Customer of such a requirement before HP processes the data, unless the law prohibits this;

3.1.2 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 Customer Personal Data shall have access to the same;

3.1.3 implement appropriate technical and organizational measures to protect against unauthorized or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer 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 Customer Personal Data and having regard to the nature of the Customer Personal Data which is to be protected.

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

3.1.5 at Customer's written request and cost, taking into account the nature of processing and the information available to the HP, assist Customer with its obligations under Articles 32 to 36 of the GDPR or equivalent provisions under applicable Data Protection and Privacy Laws; and

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

4 SUB-PROCESSING

4.1 Customer authorizes HP to transfer Customer Personal Data or give access to Customer Personal Data to members of the HP Group and third parties as Sub-processors (and permit Sub-processors to do so in accordance with Clause 4.1) for the purposes of providing the Services or other purposes identified in the 'Processing Activities' section of Attachment 1. HP shall remain responsible for its Sub-processor's compliance with the obligations of this DPA. HP shall ensure that any Sub-processors to whom HP transfers Customer Personal Data enter into written agreements with HP requiring that the Sub-processors abide by terms no less protective than those set forth in this DPA. HP shall make available to Customer the current list of Sub-processors for the Services covered by the Service Agreement.

4.2 HP can at any time and without justification appoint a new Sub-processor provided that Customer is given ten (10) days' prior notice and Customer 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 HP's reasonable opinion, such objections are legitimate, HP shall refrain from using such Sub-processor in the context of the processing of Customer Personal Data. In such cases, HP shall use reasonable efforts to (i) make available to Customer a change in HP's Services or (ii) recommend a change to the Customer's configuration or use of the Services to avoid the processing of Customer Personal Data by the objected-to Sub-processor. If HP is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, Customer may, by providing written notice to HP, terminate the Service which cannot be provided by HP without the use of the objected-to Sub-processor by providing written notice to HP.

5 PERSONAL DATA INCIDENTS

5.1 HP shall notify Customer, without undue delay, if HP becomes aware of any Personal Data Incident involving Customer Personal Data and take such steps as Customer may reasonably require, within the timescales reasonably required by Customer, to remedy the Personal Data Incident and provide such further information as Customer may reasonably require. HP reserves the right to charge an administrative fee for assistance provided under this Clause 5.1 unless and to the extent that Customer demonstrates that such assistance is required because of a failure by HP to abide by this DPA.

6 INTERNATIONAL TRANSFERS OF CUSTOMER PERSONAL DATA

6.1 HP may transfer Customer Personal Data outside the country from which it was originally collected provided that such transfer is required in connection with the Services and such transfers take place in accordance with applicable Data Protection and Privacy Laws.

6.2 European Specific Provisions

6.2.1 To the extent that Customer Personal Data is transferred from a European Country to a Relevant Country, HP makes available the transfer mechanisms listed below which shall apply, in the order of precedence as set forth in Clause 6.2.2, to any such transfers in accordance with applicable Data Protection and Privacy Laws:

6.2.1.1 HP Processor Binding Corporate Rules: HP has adopted Processor Binding Corporate Rules that cover the Customer Personal Data it processes, and warrants that:

6.2.1.1.1 the HP Group member that is party to this Data Processing Agreement is a party to and bound by the Intercompany Agreement on the Processing and Transfer of HP Customer-Owned Personal Data within the HP Group;

6.2.1.1.2 the Intercompany Agreement on the Processing and Transfer of HP Customer-Owned Personal Data within the HP Group is enforceable by Customers and Data Subjects and is available to Customer upon request;

6.2.1.1.3 it will maintain its Processor Binding Corporate Rules and will promptly notify Customer in the event that the Processor Binding Corporate Rules are no longer a valid transfer mechanism.

6.2.1.2 EU-U.S. Privacy Shield: HP's Affiliate(s) located in the United States of America, which will process Customer Personal Data for purposes of the Services are certified under EU-U.S. Privacy Shield for Customer Personal Data and HP warrants that such Affiliate(s) shall remain certified and will promptly notify Customer if a relevant Affiliate does not renew or loses the certifications, or amends the certifications so that the processing of Customer Personal Data is no longer within the scope of the certification.

6.2.1.3 EU Standard Contractual Clauses: The EU Standard Contractual Clauses are hereby incorporated in their entirety into this DPA and, to the extent applicable, HP shall ensure that its 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, the terms of the EU Standard Contractual Clauses shall prevail.

6.2.2 In the event that the Services are covered by more than one transfer mechanism, the transfer of Customer Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: 1) HP Processor Binding Corporate Rules; 2) HP's EU-U.S. Privacy Shield certification; and 3) the EU Standard Contractual Clauses.

7 AUDITS

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

Attachment 1

Details of Processing

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

Categories of Data Subjects

- Customer's employees, customers agents and subcontractors.

Types of Personal Data

The Customer Personal Data processed by HP in connection with HP's provision of the Services is determined and controlled by Customer as Data Controller and in accordance with the applicable statement of work and/or purchase/change orders, but may include as examples:

- *Contact data* – such as name, professional phone number, professional email address and professional office address;
- *Security credentials data* – such as 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 computers, printers and/or devices 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; and
- Other Personal Data provided by a Data Subject when she/he interacts in-person, online or by phone by the person, or mail with service 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

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

- 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 to Customer about the Services. Examples of administrative communications may include responses to Customer 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 Customer's information;
- verify Customer identity, 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 (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[1];

(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[2]

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[3]. 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.