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 **"CCPA"** means California Consumer Privacy Act of 2018, Cal. Civ. Code 1798.100, *et seq.*, and any related regulations, each as amended and supplemented from time to time;

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

1.3 **"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;

1.4 **"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 and includes a "business" as defined under the CCPA; 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;

1.5 **"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;

1.6 **"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 CCPA, GDPR, PIPL and any applicable regulations and national standards protecting individuals' personal information in the People's Republic of China, UK General Data Protection Regulation, UK Data Protection Act 2018, 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 and Switzerland and any amendments to or replacements for such laws and regulations;

1.7 **"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;

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

1.9 **"European Country"** means a member state of the EU, Norway, Iceland, Liechtenstein andSwitzerland;

1.10 **"European-U.S. Approved Adequacy Mechanism"** means any adequacy mechanism approved under applicable Data Protection and Privacy Laws for the transfer of Personal Data from a European Country to the U.S.;

1.11 **"EU Standard Contractual Clauses"** means the EU standard contractual clauses for the transfer of Personal Data from Data Controllers to Data Processors and from Data Processors to Data Processors foreseen in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 or its successor with any necessary amendments for Switzerland;

1.12 **"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 **"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;

1.14 **"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;

1.15 **"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;

1.16 **"PIPL"** means the Personal Information Protection Law of the People's Republic of China;

1.17 **"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;

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

1.19 **"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 or the equivalent under Swiss law or UK law and includes the U.S. as long as any such adequacy finding is limited to require use of a European-U.S. Approved Adequacy Mechanism;

1.20 **"Sell"** and **"Sale"** shall have the meaning set out in CCPA;

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

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

1.23 **"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 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.

2.6 In the event that certain aspects of the Services require activities that are deemed a Sale under CCPA each Party will be individually responsible for its own compliance with the CCPA to the extent applicable and will provide reasonable assistance to the other Party as necessary for the other Party to fulfill its obligations under the CCPA.

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 agreed between the Parties). Without limitation to the generality of the foregoing, to the extent the CCPA applies HP shall not Sell Customer Personal Data for any purpose other than the specific purpose of performing the Services. 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 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 assist Customer to fulfil the Customer's obligations under PIPL ; 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. Where PIPL applies, HP shall request Customer’s prior authorization to appoint a new Sub-processor. Customer must respond to HP’s request within ten (10) days. If Customer objects to the change, 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, including, without limitation, completing any prior assessments required by 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. HP shall maintain such HP Processor Binding Corporate Rules and promptly notify Customer in the event that the HP Processor Binding Corporate Rules are no longer a valid transfer mechanism. HP Processor Binding Corporate Rules are available on this link: https://www.hp.com/uk-en/bcr-pages.html?jumpid=in_R11928_/us/en/corp/privacy-central/binding-corporate-rules.

6.2.1.2 European-U.S. Approved Adequacy Mechanism: any transfer under a European-U.S. Approved Adequacy Mechanism must be made in accordance with the rules of the mechanism including, where required, the registration or certification of HP's Affiliate(s) located in the United States of America, which will process Customer Personal Data for purposes of the Services.

6.2.1.3 EU Standard Contractual Clauses, either Data Controller to Data Processor (Attachment 2) or Data Processor to Data Processor (Attachment 3), as applicable.

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) European U.S. Approved Adequacy Mechanism; 3) EU Standard Contractual Clauses.

6.3 Other Specified Transfer Mechanisms

6.3.1 Without prejudice to the generality of Clause 6.1 above, the Parties agree that the transfer mechanisms referred to in Attachment 4 (UK) and 5 (Argentina) shall be used to transfer Personal Data from the country in question to a Relevant Country.

6.4 China Specific Provisions

6.4.1 To the extent that any Customer Personal Data that is collected or generated within China is transferred from the People's Republic of China by HP to a country or region outside of China, HP makes available the transfer mechanisms listed below:

6.4.1.1 The security assessment: where the security assessment conducted by the Cyberspace Administration of China (CAC) applies to the transfer of Customer Personal Data, the Customer shall apply for the security assessment and comply with the relevant requirement and HP shall provide assistance if necessary.

6.4.1.2 Standard Contract (Attachment 6): where the security assessment does not apply, the Customer must enter into a standard contract published by the CAC, with the recipient of the Customer Personal Data.

6.4.2 Where the Data Controller transfers Personal Data from the People's Republic of China to the Data Processor in a country or region outside of China, the Data Controller shall be responsible for getting data subjects' consent to the transfer.

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 shall not 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 or personal phone number, professional or personal email address and professional office address;
- *Security credentials data* – such as employee identification or badge number;
- *Product usage data* – such as pages printed, types of devices that initiated print jobs, 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 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, 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; or (ii) on devices received by HP.

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 viewing and managing data, managing devices, 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, product usage or performance reports, 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; and
- wipe data from devices returned to HP.

Attachment 2

EU STANDARD CONTRACTUAL CLAUSES (DATA CONTROLLER TO DATA PROCESSOR)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

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

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

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

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons

authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

(a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(d) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 90 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a

processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that

respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

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

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of France.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

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

Name: See Customer's name in the Agreement

Address: See Customer's address in the Agreement

Contact person's name, position and contact details: See Customer's contact person's name, position and contact details in the Agreement

Activities relevant to the data transferred under these Clauses: Same as the Agreement

Signature and date: Same as the Agreement

Role (controller/processor): Controller

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

Name: See HP's name in the Agreement

Address: See HP's address in the Agreement

Contact person's name, position and contact details: Zoe McMahon, DPO, https://www.hp.com/us-en/privacy/ww-privacy-form.html

Activities relevant to the data transferred under these Clauses: Same as the Agreement

Signature and date: Same as the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Attachment 1.

Categories of personal data transferred

See Attachment 1.

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

See attachment 1.

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

See attachment 1.

Nature of the processing

See attachment 1.

Purpose(s) of the data transfer and further processing

See attachment 1.

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

See Agreement and DPA.

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

Subject matter: See Attachment 1.

Nature: See Attachment 1.

Duration of the processing: As long as the contract is in effect.

C. COMPETENT SUPERVISORY AUTHORITY

ANNEX II

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

To protect Customer data, HP abides by a robust set of information security controls including policies, practices, procedures, and organizational structures to safeguard the confidentiality, integrity, and availability of its own and its customers' information (including Personal Data as defined in HP's Customer and Data Processing Addenda). The following sets forth an overview of HP's technical/organizational security measures throughout the company.

1. Security Policy

HP maintains globally applicable policies, standards, and procedures intended to protect HP and Customer data. The detail of HP's security policies is confidential to protect the integrity of HP's data and systems. However, summaries of our key policies are included below.

2. Information Security Organization

HP has an Information Security Organization responsible for directing and managing the organization's information security strategy and controls. An Information Security Framework/Management System is put in place to ensure compliance with HP's security policies and controls and confirm that the security requirements of its customers are complied with. This Framework is structured in alignment with the NIST Cybersecurity Framework and is reviewed annually.

3. Asset Management

HP has a process in place for identifying technical information assets, and through this process, HP identifies all assets under its responsibility and categorizes the critical assets. HP further maintains a set of documented handling procedures for each information classification type, including those assets that contain Personal Data. Handling procedures address storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification.

4. Access Control

The principle of least privilege is used for providing logical access control. User access is provided via a unique user ID and password. HP's password policy has defined complexity, strength, validity, and password-history related controls. Access rights are reviewed periodically and revoked upon personnel departure.

User account creation and deletion procedures, as have been mutually agreed upon, are implemented to grant and revoke access to client systems used during the engagement.

5. Personnel Training

HP employees must complete the Integrity at HP training designed to ensure that employees are familiar with the program, policies, and resources that govern HP's expectations for ethical behavior, excellence, and compliance. Integrity at HP features modules on security and data privacy, and employees also are required to take an annual "refresher" course. HP employees must also complete an annually refreshed dedicated security awareness training focused on essential security policies and emphasizing the employees' responsibilities related to incident management, data privacy, and information security.

6. Third Parties and Subcontractors

HP has processes in place to select sub-contractors that are able to comply with comprehensive contractual security requirements.

For applicable suppliers (suppliers that handle/store/transmit HP data and customer owned HP held data or have access to the HP network), HP Cybersecurity performs a risk assessment to verify the existence of an information security program. An adequate program must include physical, technical, and administrative safeguards. This assessment must be done before the supplier has access to HP information.

7. Systems Security

By policy, the development of systems and supporting software within HP follow a secure development methodology to ensure security throughout the system/software lifecycle. The Software Development Lifecycle defines initiation, development/acquisition, implementation, operations, and disposal

requirements. All system components, including modules, libraries, services, and discrete components, are evaluated to determine their impact on the overall system security state.

HP has defined controls for the protection of application service transactions. These controls include validating and verifying user credentials, mandating digital signatures and encryption, implementing secure communication protocols, storing online transaction details on servers within the appropriate network security zone.

Internal vulnerability scans are performed regularly.

8. Physical and Environmental Security

HP facilities are secured using various physical and electronic access controls and surveillance capabilities. Depending on the facility, this could include security guards, electronic access control, and closed-circuit television (CCTV).

All HP personnel are registered and are required to carry appropriate identification badges.

Facilities have required infrastructure support with temperature control and power backups where required, using UPS and/or diesel generators to support critical services.

9. Operations Management

HP has defined a minimum set of hardening requirements for technology infrastructure, including workstations, servers, and network equipment. Workstation/servers images contain pre-hardened operating systems. Hardening requirements vary depending on the type of operating system and applicable controls implemented.

HP has deployed Network Intrusion Detection/Prevention Systems (NIDS/ NIPS) within the network and are monitored and managed 24*7.

HP security policies and standards mandate secure disposal of media.

10. Cryptography

HP has defined a set of robust processes for cryptography to ensure the confidentiality, integrity, and availability of information assets. Approved protocols require encryption for certain assets, including those that contain personal data.

11. Information Security Incident Management

HP follows a developed Cyber Incident Management Process that addresses purpose, scope, roles, responsibilities, management commitment, organizational coordination, implementation procedures, and compliance checking. HP reviews and updates this process on an annual basis.

A Cyber Incident Response Team, which includes HP Cybersecurity personnel trained in incident response and crisis management, is assembled for regular table-top reviews of process and any incident or event.

12. Business Continuity Management

HP maintains a global Continuity of Operations program. This program takes a holistic, company-wide approach for end-to-end continuity through a set of collaborative, standardized, and internally documented planning processes.

HP periodically exercises its business continuity plans to ensure their effectiveness. HP currently tests and updates all plans at least yearly and ensures that people with a role in the business continuity plan are trained.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Sub-processors only process: name, business email address, business phone number, business address. The purpose of transferring this data is to complete the contract.

For HP all of the above technical and organizational measures are flowed down to the sub-processors through the partner code of conduct and contract terms. Sub-processors are required to commit to following HP's requirements.

Attachment 3

EU STANDARD CONTRACTUAL CLAUSES (DATA PROCESSOR TO DATA PROCESSORS)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

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

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

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

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter

shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

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

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of France.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

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

Name: See Customer's name in the Agreement

Address: See Customer's address in the Agreement

Contact person's name, position and contact details: See Customer's contact person's name, position and contact details in the Agreement

Activities relevant to the data transferred under these Clauses: Same as the Agreement

Signature and date: Same as the Agreement

Role (controller/processor): Processor

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

Name: See HP's name in the Agreement

Address: See HP's address in the Agreement

Contact person's name, position and contact details: Zoe McMahon, DPO, https://www.hp.com/us-en/privacy/ww-privacy-form.html

Activities relevant to the data transferred under these Clauses: Same as the Agreement

Signature and date: Same as the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Attachment 1

Categories of personal data transferred

See Attachment 1.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation,

access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See attachment 1.

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

See attachment 1.

Nature of the processing

See Attachment 1.

Purpose(s) of the data transfer and further processing

See attachment 1.

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

See Agreement and DPA.

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

Subject matter: See Agreement 1.

Nature: See Agreement 1.

Duration of the processing: As long as the contract is in effect.

C. COMPETENT SUPERVISORY AUTHORITY

Commission Nationale de l'informatique et des Libertés (CNIL)

ANNEX II

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

To protect Customer data, HP abides by a robust set of information security controls including policies, practices, procedures, and organizational structures to safeguard the confidentiality, integrity, and availability of its own and its customers' information (including Personal Data as defined in HP's Customer and Data Processing Addenda). The following sets forth an overview of HP's technical/organizational security measures throughout the company.

1. Security Policy

HP maintains globally applicable policies, standards, and procedures intended to protect HP and Customer data. The detail of HP's security policies is confidential to protect the integrity of HP's data and systems. However, summaries of our key policies are included below.

2. Information Security Organization

HP has an Information Security Organization responsible for directing and managing the organization's information security strategy and controls. An Information Security Framework/Management System is put in place to ensure compliance with HP's security policies and controls and confirm that the security requirements of its customers are complied with. This Framework is structured in alignment with the NIST Cybersecurity Framework and is reviewed annually.

3. Asset Management

HP has a process in place for identifying technical information assets, and through this process, HP identifies all assets under its responsibility and categorizes the critical assets. HP further maintains a set of documented handling procedures for each information classification type, including those assets that contain Personal Data. Handling procedures address storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification.

4. Access Control

The principle of least privilege is used for providing logical access control. User access is provided via a unique user ID and password. HP's password policy has defined complexity, strength, validity, and password-history related controls. Access rights are reviewed periodically and revoked upon personnel departure.

User account creation and deletion procedures, as have been mutually agreed upon, are implemented to grant and revoke access to client systems used during the engagement.

5. Personnel Training

HP employees must complete the Integrity at HP training designed to ensure that employees are familiar with the program, policies, and resources that govern HP's expectations for ethical behavior, excellence, and compliance. Integrity at HP features modules on security and data privacy, and employees also are required to take an annual "refresher" course. HP employees must also complete an annually refreshed dedicated security awareness training focused on essential security policies and emphasizing the employees' responsibilities related to incident management, data privacy, and information security.

6. Third Parties and Subcontractors

HP has processes in place to select sub-contractors that are able to comply with comprehensive contractual security requirements.

For applicable suppliers (suppliers that handle/store/transmit HP data and customer owned HP held data or have access to the HP network), HP Cybersecurity performs a risk assessment to verify the existence of an information security program. An adequate program must include physical, technical, and administrative safeguards. This assessment must be done before the supplier has access to HP information.

7. Systems Security

By policy, the development of systems and supporting software within HP follow a secure development methodology to ensure security throughout the system/software lifecycle. The Software Development Lifecycle defines initiation, development/acquisition, implementation, operations, and disposal requirements. All system components, including modules, libraries, services, and discrete components, are evaluated to determine their impact on the overall system security state.

HP has defined controls for the protection of application service transactions. These controls include validating and verifying user credentials, mandating digital signatures and encryption, implementing secure communication protocols, storing online transaction details on servers within the appropriate network security zone.

Internal vulnerability scans are performed regularly.

8. Physical and Environmental Security

HP facilities are secured using various physical and electronic access controls and surveillance capabilities. Depending on the facility, this could include security guards, electronic access control, and closed-circuit television (CCTV).

All HP personnel are registered and are required to carry appropriate identification badges.

Facilities have required infrastructure support with temperature control and power backups where required, using UPS and/or diesel generators to support critical services.

9. Operations Management

HP has defined a minimum set of hardening requirements for technology infrastructure, including workstations, servers, and network equipment. Workstation/servers images contain pre-hardened operating systems. Hardening requirements vary depending on the type of operating system and applicable controls implemented.

HP has deployed Network Intrusion Detection/Prevention Systems (NIDS/ NIPS) within the network and are monitored and managed 24*7.

HP security policies and standards mandate secure disposal of media.

10. Cryptography

HP has defined a set of robust processes for cryptography to ensure the confidentiality, integrity, and availability of information assets. Approved protocols require encryption for certain assets, including those that contain personal data.

11. Information Security Incident Management

HP follows a developed Cyber Incident Management Process that addresses purpose, scope, roles, responsibilities, management commitment, organizational coordination, implementation procedures, and compliance checking. HP reviews and updates this process on an annual basis.

A Cyber Incident Response Team, which includes HP Cybersecurity personnel trained in incident response and crisis management, is assembled for regular table-top reviews of process and any incident or event.

12. Business Continuity Management

HP maintains a global Continuity of Operations program. This program takes a holistic, company-wide approach for end-to-end continuity through a set of collaborative, standardized, and internally documented planning processes.

HP periodically exercises its business continuity plans to ensure their effectiveness. HP currently tests and updates all plans at least yearly and ensures that people with a role in the business continuity plan are trained.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Sub-processors only process: name, business email address, business phone number, business address. The purpose of transferring this data is to complete the contract.

For HP all of the above technical and organizational measures are flowed down to the sub-processors through the partner code of conduct and contract terms. Sub-processors are required to commit to following HP's requirements.

Attachment 4

INTERNATIONAL DATA TRANSFER AGREEMENT (IDTA) (UK)

Part 1: Tables

Table 1: Parties and signatures

Start date	Same as in the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: See Customer's full legal name in the Agreement Trading name (if different): See Customer's trading name in the Agreement Main address (if a company registered address): See Customer's main address in the Agreement Official registration number (if any) (company number or similar identifier): See Customer's official registration number in the Agreement	Full legal name: See HP's full legal name in the Agreement Trading name (if different): See HP's trading name in the Agreement Main address (if a company registered address): See HP's main address in the Agreement Official registration number (if any) (company number or similar identifier): See HP's official registration number in the Agreement
Key Contact	Full Name (optional): See in the Agreement Job Title: See in the Agreement	Full Name (optional): See in the Agreement Job Title: See in the Agreement

	Contact details including email: See in the Agreement	Contact details including email: See in the Agreement
Importer Data Subject Contact		HP Privacy Office https://www.hp.com/us-en/privacy/ww-privacy-form.html
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the **Exporter** set out above Signed: See in the Agreement Date of signature: See in the Agreement Full name: See in the Agreement Job title: See in the Agreement	Signed for and on behalf of the **Importer** set out above Signed: See in the Agreement Date of signature: See in the Agreement Full name: See in the Agreement Job title: See in the Agreement

Table 2: Transfer Details

UK country's law that governs the IDTA:	☒ England and Wales ☐ Northern Ireland ☐ Scotland
Primary place for legal claims to be made by the Parties	☒ England and Wales ☐ Northern Ireland ☐ Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ☒ Exporter is a Controller ☐ Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: ☐ Importer is a Controller

	☒ Importer is the Exporter's Processor or Sub-Processor ☐ Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	☐ UK GDPR applies to the Importer's Processing of the Transferred Data ☒ UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data: Name of agreement: If applicable, see in the Agreement Date of agreement: If applicable, see in the Agreement Parties to the agreement: If applicable, see in the Agreement Reference (if any): If applicable, see in the Agreement **Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: Name of agreement: If applicable, see in the Agreement Date of agreement: If applicable, see in the Agreement Parties to the agreement: If applicable, see in the Agreement Reference (if any If applicable, see in the Agreement **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: Name of agreement: If applicable, see in the Agreement Date of agreement: If applicable, see in the Agreement Parties to the agreement: If applicable, see in the Agreement Reference (if any): If applicable, see in the Agreement
Term	The Importer may Process the Transferred Data for the following time period: ☒ the period for which the Linked Agreement is in force

	☐ time period: ☐ (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	☒ the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. ☐ the Parties can end the IDTA before the end of the Term by serving: months' written notice, as set out in Section 29. (How to end this IDTA without there being a breach).
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: ☒ Importer ☒ Exporter ☐ neither Party
Can the Importer make further transfers of the Transferred Data?	☒ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). ☐ The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1**Error! Reference source not found.** (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ☐ if the Exporter tells it in writing that it may do so. ☐ to: ☐ to the authorised receivers (or the categories of authorised receivers) set out in: ☒ there are no specific restrictions.
Review Dates	☐ No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data

	First review date: The Parties must review the Security Requirements at least once: ☐ each month(s) ☐ each quarter ☐ each 6 months ☐ each year ☐ each year(s) ☒ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: ☒ The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: ☐ racial or ethnic origin ☐ political opinions ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic data ☐ biometric data for the purpose of uniquely identifying a natural person ☐ physical or mental health ☐ sex life or sexual orientation ☐ criminal convictions and offences ☒ none of the above ☐ set out in:

	And: ☒ The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Relevant Data Subjects	The Data Subjects of the Transferred Data are: ☒ The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Purpose	☐ The Importer may Process the Transferred Data for the following purposes: ☐ The Importer may Process the Transferred Data for the purposes set out in the Agreement. In both cases, any other purposes which are compatible with the purposes set out above. ☒ The purposes will update automatically if the information is updated in the Linked Agreement referred to. ☐ The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Table 4: Security Requirements

Security of Transmission	HP has defined controls for the protection of application service transactions. These controls include: validating and verifying user credentials, mandating digital signatures and encryption, implementing secure communication protocols, storing online transaction details on servers within the appropriate network security zone.

Security of Storage	HP's cybersecurity department/organization and HP's legal department maintain a set of documented handling procedures for each information classification type and work along with department in charge of Data Privacy for any pertinent matters. Handling procedures account for: storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification. HP Information Technology have a process in place for identifying technical information assets. HP identifies all assets under its responsibility, categorizing the critical assets. A record of information assets and systems that are both HP-owned and externally managed by service providers is maintained. Documented processes for server decommissioning, orphaned and legacy media are also implemented to ensure proper management and disposition of non-removable media.
Security of Processing	By policy, development of systems and supporting software within HP follow a secure development methodology to ensure security throughout the system/software lifecycle. The Software Development Lifecycle defines initiation, development/acquisition, implementation, operations, and disposal requirements. All system components, which include modules, libraries, services, and discrete components, are evaluated to determine their impact on the overall system security state. HP implements logging mechanisms for system applications and devices. HP has developed robust procedures for the installation, configuration, upgrade, testing, and security patching of operational software, including but not limited to email, office productivity suites, and Internet browsers. Internal vulnerability scans are performed both on a quarterly basis and after any significant change.
Organisational security measures	To protect its own as well as Customer Personal Data, HP has defined a minimum set of hardening requirements for technology infrastructure which includes workstations, servers and network equipment. Workstation / servers images contain pre-hardened operating systems. Hardening requirements vary depending on the type of operating system and applicable controls implemented. Systems with external connections will be protected by hardening and firewalls. Externally facing systems will be placed in a Demilitarized Zone (DMZ) or other similar configuration to protect internal HP systems. Critical network zones are logically isolated. Remote access to devices on the HP internal network, with the exception of the email system, requires the use of HP standard VPN solution. Network Intrusion Detection / Prevention Systems (NIDS/ NIPS) are placed in strategic locations within the network and are monitored and managed 24*7. All devices that have logging capabilities, such as operating systems, databases, applications, firewalls, routers and switches are required to be configured as per HP's logging and auditing standard.

	HP security policies and standards mandate secure disposal of media.
Technical security minimum requirements	Developers are required to follow the coding standards and testing guidelines defined for the system to comply with application security requirements. Source code is required to be secured in a manner that prevents unauthorized access. Preliminary testing is performed and non-production patch testing is scheduled. Post feedback from the non-production testing, implementation on production environment is scheduled and implemented.
Updates to the Security Requirements	☒ The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. ☐ The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	
(i) Extra technical security protections	
(ii) Extra organisational protections	
(iii) Extra contractual protections	

Part 3: Commercial Clauses

Commercial Clauses	

Part 4: Mandatory Clauses

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.

Attachment 5

STANDARD CONTRACT CLAUSES (Argentina)

In accordance with the provisions of clause 6.3.1 of the Data Processing Addendum, Customer Personal Data originally collected in the Argentine Republic may be transferred, if required in connection with the services, 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),

Attachment 6
Standard Contract for Personal Information Cross-Border Transfer

For the purposes of ensuring that the activity of the overseas recipient processing personal information meets the personal information protection standards specified in the relevant laws and regulations of the People's Republic of China, and clarifying the obligations and responsibilities of the personal information handler and the overseas recipient for personal information protection, this Contract is made and entered into by and between:

Personal information handler: _____
Address: _____
Phone:_____
E-mail:_____
Contact:_____
Position:_____
Nationality:_____

and

Overseas recipient: _____
Address:_____
Phone:_____
E-mail:_____
Contact:_____
Position:_____
Nationality:_____

based on agreements through negotiations, for compliance by both parties.

The personal information handler and the overseas recipient shall carry out the activity related to the personal information cross-border transfer in accordance with the agreements set out in the "Instructions on Personal Information Cross-Border Transfer" in Annex 1 to this Contract. For the business behaviors related to the activity, the Parties agreed to conclude a commercial contract on the date indicated in the said contract.

The text of this Contract is drawn up in accordance with the provisions of the *Provisions on Standard Contract for Personal Information Cross-Border Transfer*. If there is any other agreement between the two parties, it will be described in detail in Annex II, which constitutes an integral part of this Contract.

Article 1 Definition

In this Contract, except as otherwise provided in the context:
(1) The personal information handler and the overseas recipient are hereinafter referred to individually as a "Party" and collectively as the "Parties".
(2) "Personal information" and "sensitive personal information" have the same meaning as the those in the *Personal Information Protection Law of the People's Republic of China*.
(3) "Personal information subject" refers to a natural person identified by or associated with the personal information.
(4) The meaning of "personal information handler" is the same as that stipulated in the *Personal Information Protection Law of the People's Republic of China*.
(5) "Overseas recipient" refers to an organization or individual located outside the territory of the People's Republic of China and receiving personal information from the personal information handler.
(6) "Regulatory authority" refers to the cyberspace departments at or above the provincial level of the People's Republic of China.
(7) "Relevant laws and regulations" refer to the laws, regulations and departmental rules of the People's Republic of China, such as the *Civil Code of the People's Republic of China*, the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the people's Republic of China*, and the *Provisions on Standard Contract for Personal Information Cross-border*, as well as the laws, regulations and departmental rules that amend, modify or supplement the above-mentioned laws and regulations and departmental rules, including follow-up laws and regulations and departmental rules that replace the original laws and regulations and departmental rules.

(8) The meanings of other undefined terms in this Contract shall be consistent with those stipulated in relevant laws and regulations.

Article 2 Obligations of personal information handler

The personal information handler hereby represents, warrants, and undertakes as follows:

(1) Personal information is collected and used in accordance with relevant laws and regulations; the scope of personal information to be transferred abroad is limited to the minimum scope required to achieve the purpose of processing.
(2) Personal information subjects have been informed of the name and the contact information of the overseas recipient, the relevant information in Annex I "Instructions on Personal Information Cross-Border Transfer", as well as the methods and procedures for exercising the rights of the personal information subjects, and individuals' separate consent has been obtained, except where it is not necessary to obtain individuals' separate consent according to relevant laws and regulations; in case of involving sensitive personal information, the personal information subjects have been informed of the necessity of transferring sensitive personal information and its impact on individuals; in case of involving the personal information of juveniles under the age of 14, the consent of the parents or other guardians of the juveniles has been obtained; where a written consent is required according to laws or administrative regulations, written consent has been obtained, except where written consent is not required according to relevant laws and regulations.
(3) Personal information subjects have been informed that it and the overseas recipient have agreed through this Contract that the personal information subjects are the third-party beneficiary, and if the personal information subjects do not explicitly refuse within 30 days, they can enjoy the rights of the third-party beneficiary in accordance with this Contract.
(4) Reasonable efforts have been made to ensure that the overseas recipient can fulfill its/his obligations under this Contract and adopt the following technical and management measures (based on a comprehensive consideration of personal information security risks that may be brought about by the type, volume, scope and sensitivity of personal information, scale and frequency of transfer, the period of personal information transmission, the period of storage by the overseas recipient, and the purpose of personal information processing): see Annex III.
(5) It will provide a copy of relevant legal provisions and technical standards to the overseas recipient at its/his request.
(6) It will respond to inquiries from regulatory authorities about the personal information processing activity of the overseas recipient, except where the Parties agree that it is the overseas recipient that replies; under such circumstance, if the overseas recipient fails to reply within a specified time limit for a reply, the personal information handler will, based on the information reasonably available to it/him, still reply within a reasonable period of time.
(7) An impact assessment on personal information protection has been carried out in accordance with relevant laws and regulations on the proposed activity of providing the overseas recipient with personal information. The assessment has taken into account:

1. The legitimacy, justifiability and necessity of the purpose, scope, method, etc. of processing personal information by the personal information handler and the overseas recipient;
2. The volume, scope, types and sensitivity of personal information to be transferred abroad, and the risks that the cross-border transfer of personal information may bring to personal information rights and interests;

3. The responsibilities and obligations undertaken by the overseas recipient, and whether the management and technical measures, capabilities, etc. to fulfill the obligations can ensure the security of personal information to be transferred abroad;

4. The risk of personal information being divulged, damaged, tampered with and abused after cross-border transfer, whether the channels for individuals to safeguard personal information rights and interests are unobstructed, etc.;

5. Evaluate the possible impact of local personal information protection policy and regulations on compliance with the terms of this Contract in accordance with Article 4 of this Contract;

6. Other matters that may impact the security of personal information cross-border transfer; The personal information protection impact assessment reports shall be kept for at least three years.

(8) It will provide a copy of this Contract to the personal information subjects at their requests. To the extent necessary to protect trade secrets or other confidential information (such as the contents of protected intellectual property, etc.), the relevant contents of this Contract may be properly shielded before a copy is provided, however, it undertakes to provide an effective summary to the personal information subjects to help them understand the contents of this Contract.

(9) It bears the burden of proof to prove that the obligations under this Contract have been fulfilled.

(10) It will provide the regulatory authorities with the information specified in Paragraph (10) of Article 3, including all audit results, in accordance with relevant laws and regulations.

Article 3 Obligations of overseas recipient

The overseas recipient hereby states, guarantees and undertakes as follows:

(1) Process personal information in accordance with the agreements listed in Annex I "Instructions on Personal Information Cross-Border Transfer", unless the prior consent of the personal information subjects is obtained.

(2) It/he will provide a copy of this Contract to the personal information subjects according to their requirements. To the extent necessary to protect trade secrets or other confidential information (such as the contents of protected intellectual property, etc.), the relevant contents of this Contract may be properly shielded before a copy is provided, however, it/he undertakes to provide an effective summary to the personal information subjects to help them understand the content of this Contract. (3) The scope of personal information to be transferred abroad is limited to the minimum scope required to achieve the purpose of processing.

(4) The storage period of personal information shall be the minimum time necessary for the purpose of processing; after the above storage period is exceeded, the personal information (including all backups) shall be deleted or anonymized, unless the separate consent of the personal information subjects on the storage period is obtained. When entrusted by the personal information handler to process the personal information, provide the personal information handler with the relevant audit report after deletion or anonymization.

(5) Ensure the security of personal information processing in the following methods:

1. Take effective technical and management measures to ensure the security of personal information, including preventing personal information from accidental or illegal destruction, loss, tampering, unauthorized provision or access (hereinafter referred to as "data disclosure"). In order to fulfil this obligation, the technical and management measures provided for in Article 2 (4) are taken. Conduct inspections on a regular basis to ensure that these measures continue to maintain an appropriate level of safety.

2. Ensure that the personnel authorized to process personal information fulfill the obligation of maintaining confidentiality and establish an access control policy of minimum authorization so that the aforementioned personnel can only access the minimum necessary personal information

required for their duties, and have only the least data operation permissions necessary to perform their duties.

(6) If there is a data disclosure of the personal information that has been processed, it/he will:

1. Take appropriate remedial measures in a timely manner to reduce the adverse impact on the personal information subjects;

2. Notify the personal information handlers immediately and report to the regulatory authorities of the People's Republic of China in accordance with relevant laws and regulations. The notification contains the following:

(a) Reasons for a leakage of personal information;

(b) The types of personal information leaked and the harm that may be caused;

(c) Remedial measures that have been taken;

(d) Measures that individuals can take to mitigate hazards;

(e) The contact information of the person in charge of dealing with the data leakage or the responsible team.

3. Where relevant laws and regulations require the personal information subjects to be notified, the content of the notice shall include the contents of Subparagraph 2 above.

4. Record and retain all facts relating to data leakage and its impact, including all remedial measures taken;

5. When it/he is entrusted by the personal information handler to process personal information, the personal information handler shall fulfill the obligation of notifying the personal information subjects as stipulated in Subparagraph 3 above.

(7) It/he will not provide personal information to third parties located outside the People's Republic of China unless all of the following requirements are met:

1. It/he does have real business that requires a provision of personal information.

2. The personal information subjects have been informed of the identity and the contact information of the third party, the purpose of processing, the method of processing, the types of personal information, as well as the methods and procedures for exercising the rights of the personal information subjects, and individuals' separate consent has been obtained, except where it is not necessary to obtain individuals' separate consent according to relevant laws and regulations; in case of involving sensitive personal information, inform the personal information subjects of the necessity of transferring sensitive personal information and its impact on individuals; in case of involving the personal information of juveniles under the age of 14, the consent of the juveniles' parents or other guardians shall be obtained; where a written consent is required as stipulated by laws or administrative regulations, written consent shall be obtained, except where it is not necessary to obtain the written consent according to relevant laws and regulations. When it is difficult to inform or obtain separate consent of the personal information subjects, inform the personal information handler in a timely manner, and request the personal information handler to provide assistance in informing the personal information subjects or obtaining the personal information subjects' separate consent.

3. Reach a written agreement with the third party to ensure that the level of personal information protection provided by the third party is not lower than that stipulated in the relevant laws and regulations of the People's Republic of China, and bear joint and several liability that may cause damage to the personal information subjects as a result of re-provision;

4. Provide a copy of the agreement to the personal information handler.

(8) Obtain the prior consent of the personal information handler when being entrusted by it to process the personal information and entrusting it to a third party; ensure that the entrusted third party does not process personal information beyond the purpose and method of processing stipulated in Annex 1

"Instructions on Personal Information Cross-Border Transfer" to this Contract, and supervise the personal information processing activity of that third party.
(9) Make automated decisions by using personal information, ensure the transparency of decisionmaking and the fairness and impartiality of the results, and do not accord unreasonable differential treatment to individuals on transaction conditions such as transaction prices. Push information to individuals and carry out commercial marketing through automated decision-making, while providing options that are not specific to their personal characteristics, or providing a convenient way to refuse.
(10) Undertake to provide the personal information handler with all necessary information to prove compliance with the obligations under this Contract, and allow the personal information handler to view data files and documents, or audit the processing activity covered by this Contract. When the personal information handler decides to view or audit, provide facilitation for the handler to carry out the audit on its own or entrust a third party to do so, and at the handler's request, provide the personal information handler with the documents of qualification certification on the personal information protection.
(11) Keep an objective record of the personal information processing activity carried out, retain the records for at least three years, and provide relevant records and documents to the regulatory authorities directly or through the personal information handler as required by relevant laws and regulations.
(12) Agree to be subject to the supervision and administration of the regulatory authorities in the relevant procedures for supervising the implementation of this Contract, including, but not limited to, responding to the inquiries of the regulatory authorities, cooperating in the inspection of the regulatory authorities, and complying with the measures or decisions taken or made by the regulatory authorities, and providing written proof that necessary actions have been taken.

Article 4 Impact of personal information protection policy & regulations in the overseas recipient's home country/region on compliance with this Contract

(1) The Parties hereby guarantee that a lack of the knowledge of the personal information protection policy & regulations (including any requirements for the provision of personal information or the provisions authorizing public organs to access personal information) in the overseas recipient's home country/region even after reasonable efforts will prevent the overseas recipient from fulfilling its/his obligations under this Contract.
(2) The Parties hereby state that in providing the guarantee in Paragraph (1) of Article 4, the following factors have been taken into account:

1. Specific information regarding cross-border transfer, including the types, volume, scope and sensitivity of personal information to be transferred abroad, the scale and frequency of transfer, the period of personal information transmission and the storage period of the overseas recipient, the purpose of personal information processing, previous similar experience of the overseas recipient in the cross-border transfer and processing of personal information, whether data security-related incidents have occurred to the overseas recipient and whether they have been dealt with in a timely and effective manner, whether the overseas recipient ever received a request from the public organs of its/his home country/region to provide personal information and the response of the overseas recipient;
2. Personal information protection policy & regulations in the overseas recipient's home country/region include the following factors:

(a) The current laws and regulations and widely applied standards for the personal Information protection in that country or region;
(b) Regional or global organizations on personal information protection to which the country or region is a member, and binding international commitments made;

(c) The mechanism for the personal information protection in that country or region, such as whether there are supervision and law enforcement authorities and relevant judicial bodies for the personal information protection.

3. The security management system and technical means guarantee capability of the overseas recipient.

(3) The overseas recipient guarantees that in conducting an evaluation in accordance with Paragraph (2) of Article 4, it/he has made every effort to provide the personal information handler with the necessary relevant information.

(4) The Parties shall record the process and results of the evaluation conducted in accordance with Paragraph (2) of Article 4.

(5) Where the overseas recipient is unable to perform this Contract due to changes in the personal information protection policy & regulations in the overseas recipient's home country/region (including changes in the laws of the overseas recipient's home country/region, or taking compulsory measures), the overseas recipient shall notify the personal information handler immediately after being aware of the above-mentioned changes.

Article 5 Rights of personal information subjects

The Parties acknowledge that, in accordance with relevant laws and regulations, the personal information subjects are vested with the right to carry out the obligations of the Parties to protect personal information in this Contract as a third party beneficiary.

(1) Personal information subjects shall, in accordance with relevant laws and regulations, have the right to know, the right to make decisions, the right to restrict or refuse others to process their personal information, the right to view, the right to copy, the right to make corrections and supplement, and the right to delete, and the right to require an explanation of their personal information processing rules.

(2) When personal information subjects request to exercise the above-mentioned rights over the personal information that has been transferred abroad, they may request the personal information handler to take appropriate measures to achieve it, or make a request directly to the overseas recipient. If the personal information handler is unable to achieve it, it shall notify and request the overseas recipient to assist in realizing it.

(3) The overseas recipient shall, in accordance with the notification of the personal information handler or at the request of the personal information subjects, realize the rights exercised by the personal information subjects in accordance with the relevant laws and regulations within a reasonable time limit. The overseas recipient shall inform the personal information subjects truthfully, accurately and completely in a clear and plain language.

(4) If the personal information subjects make too many or unreasonable requests, especially repetitive requests, the overseas recipient may charge a reasonable fee or refuse to act in accordance with the requests after taking into account the cost of implementation and operating of the requests once they are approved.

(5) If the overseas recipient plans to reject the request of the personal information subjects, it/he shall inform the personal information subjects of the reasons for such refusal and the methods for the personal information subjects to lodge a complaint with the relevant regulatory authorities and seek judicial relief.

(6) The personal information subjects, as the third-party beneficiary under this Contract, shall have the right to claim and demand, to any of the personal information handler and the overseas recipient, the performance of the following provisions relating to the rights of the personal information subjects under this Contract:

1. Article 2, except Paragraphs (4), (5), (6) and (10) of Article 2;

2. Article 3, except Subparagraphs 2 and 4 of Paragraph (6) , Paragraphs (8), (10), (11), (12) of Article 3;
3. Article 4;
4. Article 6;
5. Article 7;
6. Paragraphs (3), (4), (6) of Article 8;
7. Paragraphs (4) and (6) of Article 9.

Article 6 Relief

(1) The overseas recipient shall appoint a contact person within the organization and authorize him to respond to inquiries or complaints about the processing of personal information, and shall handle any inquiries or complaints from the personal information subjects in a timely manner. The overseas recipient shall inform the personal information handler of the contact information, and inform the personal information subjects of the contact information through a separate notification or announcement on its/his website in a simple and easy-to-understand way, as follows: see contact person and contact information in the main contract/agreement and/or Data Processing Agreement/Data Processing Standard.
(2) The Parties agree that if a dispute between a personal information subject and either of the Parties occurs in terms of complying with this Contract, such either party shall inform the other party of the relevant situation and cooperate to resolve the dispute in a timely manner.
(3) If the dispute is not settled amicably and the personal information subject exercises the rights of the third party beneficiary in accordance with Paragraph (2) of Article 6, the overseas recipient accepts the following claims of the personal information subject:
1. Lodge a complaint with the regulatory authorities;
2. Bring an action in the court as provided for in Article 9 (4).

(4) The overseas recipient agrees that the settlement of the dispute over this Contract by the relevant personal information subjects shall be based on the relevant laws and regulations of the People's Republic of China.
(5) The overseas recipient agrees that the choice in protecting rights made by the personal information subjects will not detract from the substantive or procedural right of the personal information subject to seek relief in accordance with other laws and regulations.

Article 7 Cancellation of contract
(1) If the overseas recipient violates the obligations under this Contract, the personal information handler may suspend the transfer of personal information to the overseas recipient until the violation is corrected or this Contract is cancelled.
(2) Under any of the following circumstances, the personal information handler shall have the right to cancel this Contract and, if necessary, notify the regulatory authorities:
1. The personal information handler suspends the transfer of personal information to the overseas recipient for more than one month in accordance with Paragraph (1) of Article 7.
2. The overseas recipient's compliance with this Contract will violate the laws and regulations of its/his home country;
3. The overseas recipient seriously or continuously violates the obligations under this Contract;
4. According to the final decision of prohibiting appeals made by the competent court or regulatory authority of the overseas recipient, the overseas recipient or personal information handler has violated the provisions of this Contract;

5. Bankruptcy, dissolution or liquidation of the overseas recipient: the request for the legal dissolution of the overseas recipient, whether in the name of an individual or organization, is not rejected within the legal time limit; the overseas recipient makes the dissolution decision; the overseas recipient is appointed as the bankruptcy administrator; the overseas recipient carries out bankruptcy, dissolution or liquidation proceedings on its/his own; the overseas recipient faces a similar situation in its/his home country/region.

In the case of Subparagraphs 1, 2 or 4 above, the overseas recipient may also cancel this Contract.

(3) If the regulatory authority makes decisions related to the cross-border transfer of personal information in accordance with relevant laws and regulations, such as the security assessment on cross-border transfer of personal information, which makes this Contract unenforceable, either party may cancel this Contract.

(4) This Contract is cancelled with the consent of the Parties, but the cancellation of this Contract shall not indemnify them from their obligations to protect personal information in the process of personal information processing.

(5) Upon cancellation of this Contract, the overseas recipient shall immediately return, destroy or anonymously process the personal information received under this Contract, and provide an audit report on destruction or anonymization of personal information.

Article 8 Liability for breach of contract

(1) Either party shall be liable to the other party for any damage caused to the other party as a result of their breach of this Contract.

(2) The liability between the two parties shall be limited to the losses suffered by the non-breaching party.

(3) Each party who violates this Contract and infringes upon the rights enjoyed by the personal information subjects as a third-party beneficiary shall bear responsibility to the personal information subjects; the personal information subjects shall have the right to compensation. This does not affect the responsibility of the personal information handler under the relevant laws and regulations.

(4) If the personal information handler and the overseas recipient are responsible for any material or non-material damage jointly caused to a personal information subject as a result of the breach of this Contract, the personal information handler and the overseas recipient shall be jointly and severally liable to the personal information subject.

(5) The Parties agree that if one party (the “indemnifying party”) is jointly and severally liable to the personal information subject for the breach of this Contract by the other party (the “breaching party") and the joint and several liability of the indemnifying party exceeds its share of liability, the indemnifying party shall have the right to recover compensation from the breaching party.

(6) Notwithstanding the provisions of Paragraphs (3) and (4) of Article 8, the personal information handler shall be responsible to a personal information subject for any material and non-material losses caused by the overseas recipient to the personal information subject as a result of breach of this Contract, the personal information subject shall have the right to claim liability for damages.

(7) The Parties agree that if the personal information handler is responsible for the damage caused by the overseas recipient in accordance with Paragraph (6) of Article 8, the former shall have the right to recover compensation from the latter.

Article 9 Miscellaneous

(1) In the event of a conflict between this Contract and any other agreements already existing between the parties at the time of its conclusion, the terms of this Contract shall prevail.

(2) This Contract is governed by the relevant laws and regulations of the People's Republic of China.

(3) All notices given by one party to the other party shall be sent promptly by e-mail, telegram, telex or fascimile (a confirmed copy by airmail required) or registered air mail or be posted to the (specific address) or other address in place of such addresses by a written notice. If a notice or communication under this

Contract is sent by registered airmail, it shall be deemed to have been received 20 days after the date of the postmark, and if sent by e-mail, telegram, telex or fascimile, it shall be deemed to have been received 5 working days after it was sent out.

(4) Where the personal information subjects, as a third-party beneficiary, bring a lawsuit against the personal information handler or the overseas recipient, the jurisdiction shall be determined in accordance with the provisions of the *Civil Procedure Law of the People's Republic of China*.

(5) Any dispute arising from this Contract between the personal information handler and the overseas recipient and any party's claim for compensations from the other party for making advance compensation for the personal information subject's damages shall be settled through negotiation by both parties; if the disputes cannot be resolved, either party may take the following method litigation for settlement:

1. Arbitration. Submit the dispute to

□ China International Economic and Trade Arbitration Commission

□ China Maritime Arbitration Commission

□ Beijing Arbitration Commission (Beijing International Arbitration Center)

□ Other arbitration agency in a member state of the *Convention on the Recognition and Enforcement of Foreign Arbitral Awards*: _____. Arbitration will be conducted at _____ (place of arbitration) in accordance with its arbitration rules then in force.

2. Litigation. Bring a suit before a people's court with jurisdiction in China in accordance with the law.

(6) This Contract shall be interpreted in accordance with the provisions of relevant laws and regulations, and shall not be interpreted in a manner inconsistent with the rights and obligations stipulated in relevant laws and regulations.

(7) This Contract is made out in (see main contract/agreement and/or Data Processing Agreement/Data Processing Standard) for each party, having the same legal effect.

(8) This Contract is established after being formally signed by both parties and shall enter into force immediately.

This Contract is concluded by the personal information handler and the overseas recipient at _____.

Personal information handler: _____(seal)

Legal representative/entrusted agent: _____(signature or seal)

_____(date)

Overseas recipient: _____(seal)

Legal representative/entrusted agent: _____(signature or seal)

_____(date)

Annex I
Instructions on Personal Information Cross-Border Transfer

Details of the cross-border transfer of personal information under this Contract are agreed upon as follows:

(1) The personal information to be transferred belongs to the following categories of personal information subjects:

(2) The transfer is for the following purposes:

(3) Volume of personal information to be transferred:

(4) Categories of personal information to be transferred abroad (refer to GB/T 35273 *Information security technology - Personal information security specification* and relevant standards):

(5) Categories of sensitive personal information to be transferred abroad (if applicable, refer to GB/T 35273 *Information security technology - Personal information security specification* and relevant standards):

(6) The personal information to be transferred by the overseas recipient shall only be provided to the following recipients:

(7) Method of transfer:

(8) Storage period after cross-border transfer:

(9) Storage location after cross-border transfer:

(10) Other matters (as appropriate):

Annex II
Other Terms Agreed Upon By the Parties (If necessary)

Annex III

Technical and organizational measures

1. Organization

HP has an Information Security Organization responsible for directing and managing the organization's information security strategy and controls. An Information Security Framework/Management System is put in place to ensure compliance with HP's security policies and controls and confirm that the security requirements of its customers are complied with. This Framework is structured in alignment with the NIST Cybersecurity Framework and is reviewed annually.

2. Asset Management

HP has a process in place for identifying technical information assets, and through this process, HP identifiesall assets under its responsibility and categorizes the critical assets. HP further maintains a set of documented handling procedures for each information classification type, including those assets thatcontain Personal Data. Handling procedures address storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification.

3. Access Control

The principle of least privilege is used for providing logical access control. User access is provided via a unique user ID and password. HP's password policy has defined complexity, strength, validity, and password-history related controls. Access rights are reviewed periodically and revoked upon personnel departure.

User account creation and deletion procedures, as have been mutually agreed upon, are implemented to grant and revoke access to client systems used during the engagement.

4. Personnel Training

HP employees must complete the Integrity at HP training designed to ensure that employees are familiar with the program, policies, and resources that govern HP's expectations for ethical behavior,

excellence, and compliance. Integrity at HP features modules on security and data privacy, and employees also are required to take an annual “refresher” course. HP employees must also complete an annually refreshed dedicated security awareness training focused on essential security policies and emphasizing the employees’ responsibilities related to incident management, data privacy, and information security.

5. Third Parties and Subcontractors

HP has processes in place to select sub-contractors that are able to comply with comprehensive contractualsecurity requirements.

For applicable suppliers (suppliers that handle/store/transmit HP data and customer owned HP held data or have access to the HP network), HP Cybersecurity performs a risk assessment to verify the existence of an information security program. An adequate program must include physical, technical, and administrative safeguards. This assessment must be done before the supplier has access to HP information.

6. Systems Security

By policy, t h e development of systems and supporting software within HP follow a secure development methodology to ensure security throughout the system/software lifecycle. The Software Development Lifecycle defines initiation, development/acquisition, implementation, operations, and disposal requirements. All system components, including modules, libraries, services, and discrete components,are evaluated to determine their impact on the overall system security state.

HP has defined controls for the protection of application service transactions. These controls include validating and verifying user credentials, mandating digital signatures and encryption, implementing securecommunication protocols, storing online transaction details on servers within the appropriate network security zone.

Internal vulnerability scans are performed regularly.

7. Physical and Environmental Security

HP facilities are secured using various physical and electronic access controls and surveillance capabilities. Depending on the facility, this could include security guards, electronic access control, and closed-circuit television (CCTV).

All HP personnel are registered and are required to carry appropriate identification badges.

Facilities have required infrastructure support with temperature control and power backups where required, using UPS and/or diesel generators to support critical services.

8. Operations Management

HP has defined a minimum set of hardening requirements for technology infrastructure, including workstations, servers, and network equipment. Workstation/servers images contain pre-hardened operating systems. Hardening requirements vary depending on the type of operating system and applicable controls implemented.

HP has deployed Network Intrusion Detection/Prevention Systems (NIDS/ NIPS) within the network and aremonitored and managed 24*7.

HP security policies and standards mandate secure disposal of media.

9. Cryptography

HP has defined a set of robust processes for cryptography to ensure the confidentiality, integrity, and availability of information assets. Approved protocols require encryption for certain assets, including thosethat contain personal data.

10. Information Security Incident Management

HP follows a developed Cyber Incident Management Process that addresses purpose, scope, roles, responsibilities, management commitment, organizational coordination, implementation procedures, and compliance checking. HP reviews and updates this process on an annual basis.

A Cyber Incident Response Team, which includes HP Cybersecurity personnel trained in incident response and crisis management, is assembled for regular table-top reviews of process and any incident or event.

12. Business Continuity Management

HP maintains a global Continuity of Operations program. This program takes a holistic, company-wide approach for end-to-end continuity through a set of collaborative, standardized, and internally documentedplanning processes.

HP periodically exercises its business continuity plans to ensure their effectiveness. HP currently tests and updates all plans at least yearly and ensures that people with a role in the business continuity plan are trained.