ANNEXE TRAITEMENT DES DONNÉES PERSONNELLES DU CLIENT

La présente Annexe relative au Traitement des Données (« ATDP ») et ses Appendices s'appliquent lorsque HP traite les Données personnelles du Client afin de fournir les Services convenus dans le ou les contrats applicables entre HP et le Client (« Contrat de Services »). Les termes commençant par une majuscule qui ne sont pas définis dans le présent document ont le sens qui leur est donné dans le Contrat de Services. En cas de conflit entre les dispositions du Contrat de Services relatives au Traitement des Données Personnelles et le présent ATDP, l'ATDP prévaudra.

1 DÉFINITIONS

1.1 « **CCPA** » désigne le California Consumer Privacy Act de 2018 (loi californienne relative à la protection de la vie privée des consommateurs), tel que modifié par le California Privacy Rights Act (loi californienne relative aux droits à la protection de la vie privée) (« CPRA »), articles 1798.100 et suiv. du Code civil de Californie, *et* , toute réglementation connexe, chacune telle que modifiée et complétée le cas échéant;

1.2 « **Client** » désigne le client utilisateur final des Services HP ;

1.3 « **Données personnelles du Client** » désigne les Données à caractère personnel pour lesquelles le Client est le Responsable du traitement et qui sont traitées par HP en qualité de Sous-traitant ou par ses Sous-traitants ultérieurs dans le cadre de la fourniture des Services ;

1.4 « **Responsable de traitement** » désigne la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles et comprend une « entreprise » telle que définie par le CCPA ;

1.5 « **Sous-traitant**» désigne toute personne physique ou morale, autorité publique, agence ou tout autre organisme qui traite des Données personnelles pour le compte du Responsable du traitement ou sur instruction d'un autre Sous-traitant agissant pour le compte d'un Responsable de traitement ;

1.6 « **Lois relatives à la protection de la vie privée et des données personnelles** » désigne toutes les lois et réglementations applicables actuelles et futures relatives au traitement, à la sécurité, à la protection et à la conservation des Données personnelles et au respect de la vie privée qui peuvent exister dans les juridictions concernées, y compris, mais sans s'y limiter, le CCPA, le RGPD, PIPL et toutes les réglementations et normes nationales applicables protégeant les informations personnelles des individus en République populaire de Chine, la Réglementation générale britannique sur la protection des données, UK Data Protection Act 2018, la directive 2002/58/CE concernant le traitement des Données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, toutes les lois ou réglementations nationales mettant en œuvre les directives précédentes et toutes les lois relatives à la protection des données de la Norvège, de l'Islande, du Liechtenstein et de la Suisse ainsi que tous les amendements ou remplacements de ces lois et réglementations ;

1.7 « **Personne concernée » a le sens attribué au terme « personne concernée** » en vertu des Lois relatives à la protection de la vie privée et des données personnelles et inclut, au minimum, toutes les personnes physiques identifiées ou identifiables auxquelles les Données personnelles se rapportent ;

1.8 « **Désidentifier** » : processus qui transforme les données personnelles en données qui ne peuvent raisonnablement être utilisées pour déduire des informations sur, identifier, localiser, contacter, relier, décrire, être associées ou autrement liées, directement ou indirectement, à une personne ou un foyer particulier, ou à un appareil lié à une personne ou un foyer ;

1.9 « **UE** » désigne l'Union européenne et les pays qui en sont membres, collectivement ;

1.10 « **Pays européen** » désigne un État membre de l'UE, la Norvège, l'Islande, le Liechtenstein et de la Suisse;

1.11 « Mécanisme de conformité approuvé par l'Europe et les États-Unis » désigne tout mécanisme de conformité approuvé en vertu des Lois relatives à la protection de la vie privée et des données personnelles pour le transfert de Données personnelles d'un Pays européen vers les États-Unis ;

1.12 « Clauses contractuelles types de l'UE » désigne les clauses contractuelles types de l'UE pour le transfert de Données personnelles entre les Responsables du traitement des données au Sous-traitants, et des Sous-traitants aux Sous-traitants prévues dans la décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 ou son successeur ; avec les modifications nécessaires pour la Suisse ;

1.13 « RGPD » désigne le Règlement Général sur la Protection des Données (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des Données à caractère personnel et à la libre circulation de ces données ;

1.14 « Groupe HP » désigne HP Inc. (1501 Page Mill Road, Palo Alto, CA 94304, USA) et toutes ses filiales détenues et contrôlées majoritairement, quelle que soit leur juridiction de constitution ou d'exploitation ;

1.15 « Données à caractère personnel » ou « Données personnelles » désigne toute information relative à une personne physique identifiée ou identifiable ou telle qu'autrement définie par les Lois relatives à la protection de la vie privée et des Données personnelles. Une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques à son identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale ;

1.16 « Incident relatif aux Données personnelles » a le sens attribué par les Lois relatives à la protection de la vie privée et des données personnelles aux termes « incident de sécurité », « faille de sécurité » ou «violation de données personnelles », mais inclut toute situation dans laquelle HP apprend que les Données personnelles du Client ont été ou sont susceptibles d'avoir été consultées, divulguées, altérées, perdues, détruites ou utilisées par des personnes non autorisées, de manière non autorisée ;

1.17 « PIPL » désigne la loi sur la Protection des informations personnelles de la République populaire de Chine

1.18 Les termes « traiter », « traite », « traitement » ou « traité » désignent toute opération ou ensemble d'opérations effectuées sur des Données personnelles, que ce soit ou non par des moyens automatisés, y compris, sans s'y limiter, l'accès, la collecte, l'enregistrement, l'organisation, la structuration, la conservation, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, l'alignement, la combinaison, le blocage, la limitation, l'effacement et la destruction des Données personnelles et toute définition équivalente dans les Lois relatives à la protection de la vie privée et des données personnelles dans la mesure où ces définitions sont plus larges que la présente définition ;

1.19 « Règles d'entreprise contraignantes pour les Sous-traitants » désigne les règles d'entreprise contraignantes pour Sous-traitants approuvées par certaines autorités de protection de la vie privée dans l'UE ;

1.20 « Pays concerné » : désigne tous les pays autres que les pays européens et les autres pays pour lesquels il existe une décision d'adéquation en vertu de l'article 45 du RGPD ou l'équivalent en vertu des lois applicables ;

1.21 « Vendre » et « Vente » ont le sens qui leur est donné dans le CCPA ;

1.22 « Partager » a le sens qui lui est donné dans le CCPA ;

1.23 « Services » désigne les services, y compris les produits et l'assistance, fournis par HP dans le cadre du Contrat de Services ;

1.24 « Contrat de Services » désigne le contrat conclu entre HP et le Client pour l'achat de Services auprès d' HP ; et

1.25 « Sous-traitant» désigne toute personne physique ou morale, autorité publique, agence ou tout autre organisme qui traite des Données personnelles pour le compte d'un Sous-traitant agissant pour le compte d'un Responsable de traitement.

2 PORTÉE ET CONFORMITÉ AVEC LA LOI

2.1 Le présent ATDP s'applique au Traitement des Données personnelles du Client par HP dans le cadre de sa fourniture de Services et lorsque HP agit en qualité de Sous-traitant pour le compte du Client lui-même Responsable de traitement. Toutes les Parties se conforment aux obligations qui leur sont applicables en vertu de toutes les Lois relatives à la protection de la vie privée et des données personnelles. Aucune disposition du présent paragraphe 2.1 ne modifie les restrictions applicables aux droits de l'une ou l'autre des Parties d'utiliser ou de traiter autrement les Données personnelles en vertu du Contrat de Services entre les.

2.2 Les catégories de Personnes Concernées, les types de Données personnelles du Client traitées et les finalités du traitement sont indiqués dans l'Appendice1 du présent ATDP. HP traite les Données personnelles du Client pendant la durée du Contrat de Services (ou plus longtemps si la loi applicable l'exige).

2.3 Le Client, dans le cadre de son utilisation des Services HP, est seul responsable du respect de toutes les Lois relatives à la protection de la vie privée et des données personnelles en ce qui concerne l'exactitude, la qualité et la légalité des Données personnelles qui doivent être traitées par HP dans le cadre des Services. Le Client veillera en outre à ce que les instructions qu'il fournit à HP en ce qui concerne le traitement de ses Données personnelles soient conformes à toutes les Lois relatives à la protection de la vie privée et des Données personnelles et ne mettent pas HP en infraction à ses obligations en vertu de ces lois.

2.4 Si le Client utilise les Services pour traiter des catégories de Données personnelles qui ne sont pas expressément couvertes par le présent ATDP, le Client agit à ses propres risques et HP ne sera pas responsable des éventuels défauts de conformité liés à cette utilisation.

2.5 Lorsque HP divulgue au Client des Données personnelles d'un employé de HP ou qu'un employé de HP fournit directement au Client des Données personnelles que le Client traite pour gérer son utilisation des Services, le Client traite ces Données personnelles conformément à ses politiques de confidentialité et aux Lois relatives à la protection de la vie privée et des données personnelles. HP ne divulguera ces informations que dans la mesure où elles sont légitimes aux fins de la gestion des contrats, de la gestion des services ou des objectifs raisonnables du Client en matière de sécurité ou de vérification des antécédents.

3 OBLIGATIONS DU SOUS-TRAITANT

3.1 Nonobstant toute disposition contraire dans le Contrat de Services, en ce qui concerne les Données personnelles du Client, HP doit :

3.1.1 traiter les Données personnelles du Client uniquement conformément aux instructions documentées du Client (qui peuvent être de nature spécifique ou générale, comme indiqué dans le Contrat de services ou comme convenu autrement entre les Parties). Sans limiter la portée générale de ce qui précède, dans la mesure où la CCPA s'applique aux Données personnelles du Client, HP ne doit pas, d'une manière incompatible avec la CCPA : Vendre ou partager les Données personnelles du Client ; conserver, utiliser ou divulguer les Données personnelles du Client à des fins autres que les fins commerciales spécifiques liées à l'exécution des Services ou à l'exécution des obligations prévues dans le Contrat, lesquelles fins s'inscrivent dans le cadre de la relation commerciale directe entre les Parties ; ou combiner les Données personnelles du Client avec des Données personnelles provenant de toute autre source. HP ne conservera ni n'utilisera les Données personnelles du Client ou les Données personnelles anonymisées du Client à d'autres fins, y compris, mais sans s'y limiter, à ses propres fins, à des fins de réidentification ou à des fins indépendantes des obligations de HP. Dans la mesure où la CPPA s'applique aux Données personnelles du Client, HP informera le Client si elle ne peut pas respecter ses obligations en vertu de la CCPA concernant les Données personnelles du Client. Nonobstant ce qui précède, HP peut traiter les Données personnelles du Client conformément à la législation applicable. Dans ce cas, HP prendra toutes les mesures raisonnables pour informer le Client de cette exigence avant de traiter les données, sauf si la loi l'interdit ;

3.1.2 veiller à ce que l'accès soit restreint aux seuls membres du personnel autorisés qui ont suivi une formation appropriée en matière de protection et de traitement des Données personnelles et qui sont liés par l'obligation de respecter la confidentialité des Données personnelles du Client ;

3.1.3 mettre en œuvre des mesures techniques et organisationnelles appropriées pour se protéger contre la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés ou illicites des Données personnelles du Client. Ces mesures doivent être proportionnées au préjudice qui pourrait résulter d'un traitement non autorisé ou illégal, d'une perte accidentelle, d'une destruction, d'un dommage ou d'un vol des Données personnelles du Client et tenir compte de la nature des Données personnelles du Client à protéger ;

3.1.4 sans délai injustifié et dans la mesure où la loi le permet, notifier au Client toute demande émanant de Personnes Concernées cherchant à exercer leurs droits en vertu des Lois relatives à la protection de la vie privée et des données personnelles et, sur demande écrite du Client et à ses frais, en tenant compte de la nature du traitement, aider le Client en mettant en œuvre des mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour l'aider à remplir son obligation de répondre à ces demandes ;

3.1.5 sur demande écrite du Client et à ses frais, en tenant compte de la nature du traitement et des informations dont dispose HP, aider le Client à remplir ses obligations en vertu des articles 32 à 36 du RGPD ou des dispositions équivalentes en vertu des Lois relatives à la protection de la vie privée et des données personnelles, pour aider le Client à remplir les obligations du Client au titre de la PIPL ; et les obligations au titre du CPRA ;

3.1.6 sur demande écrite du Client, supprimer ou restituer au Client toutes Données personnelles à la fin de la fourniture des Services, à moins que la législation applicable n'exige la conservation des Données à caractère personnel du Client et au choix de HP entre la suppression et la restitution des Données personnelles du Client.

4 SOUS-TRAITANCE ULTERIEUR

4.1 Le Client autorise HP à transférer ses Données personnelles ou à donner accès à ses Données personnelles aux membres du Groupe HP et à des tiers agissant en qualité de Sous-traitants ultérieurs (et à autoriser également les Sous-traitants ultérieurs à le faire conformément à la clause 4.1) aux fins de fournir les Services ou pour d'autres finalités identifiées dans le paragraphe « Activités de traitement » de l'Appendice 1. HP reste responsable du respect par ses Sous-traitants ultérieurs des obligations du présent ATDP. HP veillera à ce que les Sous-traitants ultérieurs auxquels elle transfère les Données

personnelles du Client concluent avec elle des accords écrits exigeant que les Sous-traitants ultérieurs respectent des conditions aussi protectrices que celles énoncées dans le présent ATDP. HP met à la disposition du Client la liste actualisée des Sous-traitants ultérieurs pour les Services couverts par le Contrat de Services.

4.2 HP peut à tout moment et sans justification désigner un nouveau Sous-traitant ultérieur, à condition que le Client en soit informé dix (10) jours à l'avance et que le Client ne s'oppose pas légitimement à ce changement dans ce délai. Les objections légitimes doivent contenir des motifs raisonnables et documentés relatifs au non-respect par un Sous-traitant ultérieur des Lois relatives à la protection de la vie privée et des données personnelles. Si, de l'avis raisonnable de HP, ces objections sont légitimes, HP s'abstiendra de recourir à ce sous-traitant dans le cadre du traitement des Données personnelles du Client. Dans de tels cas, HP déploiera des efforts raisonnables pour (i) mettre à la disposition du Client une modification des Services HP ou (ii) recommander une modification de la configuration ou de l'utilisation des Services par le Client afin d'éviter le Traitement des Données personnelles du Client par le Sous-traitant ultérieur visé par l'objection. Si HP n'est pas en mesure d'apporter ce changement dans un délai raisonnable, qui n'excède pas quatre-vingt-dix (90) jours, le Client peut, après en avoir informé HP par écrit, résilier le Service qui ne peut être fourni par HP sans recours au Sous-traitant ultérieur faisant l'objet d'une objection. Si la PIPL s'applique, HP doit demander l'autorisation préalable du Client pour nommer un nouveau Sous-traitant. Le Client doit répondre à la demande de HP dans un délai de dix (10) jours. Si le Client s'oppose au changement, HP doit s'abstenir de recourir à un tel Sous-traitant dans le cadre du traitement des Données personnelles du Client. Dans de tels cas, HP doit déployer des efforts raisonnables pour (i) mettre à la disposition du Client une modification des Services de HP ou (ii) recommander une modification de la configuration du Client ou de l'utilisation des Services pour éviter le traitement des Données personnelles du Client par le Sous-traitant objet de l'opposition. Si HP est dans l'incapacité de mettre à disposition une telle modification dans un délai raisonnable, qui ne saurait dépasser quatre-vingt-dix (90) jours, le Client peut, par notification écrite de HP, résilier le Service qui ne peut pas être fourni par HP sans recourir au Sous-traitant objet de l'opposition.

5 INCIDENTS RELATIFS AUX DONNÉES PERSONNELLES

5.1 HP informera le Client, sans délai injustifié, si elle a connaissance d'un Incident relatif aux Données personnelles impliquant les Données personnelles du Client et prendra les mesures que celui-ci peut raisonnablement exiger, dans un délai raisonnable, pour remédier à l'Incident relatif aux Données personnelles et fournir les informations supplémentaires que le Client peut raisonnablement exiger. HP se réserve le droit de facturer des frais administratifs pour l'assistance fournie en vertu de la présente clause 5.1, sauf si, et dans la mesure où, le Client démontre que cette assistance est nécessaire en raison d'un manquement de HP au présent ATDP.

6 TRANSFERTS INTERNATIONAUX DES DONNÉES PERSONNELLES DU CLIENT

6.1 HP peut transférer les Données personnelles du Client en dehors du pays dans lequel elles ont été collectées à l'origine, à condition que ce transfert soit nécessaire dans le cadre des Services et que ce transfert ait lieu conformément aux Lois relatives à la protection de la vie privée et des données personnelles, y compris, mais sans s'y limiter, mener toute évaluation préalable requise par les Lois relatives à la protection de la vie privée et des données.

6.2 Dispositions spécifiques à l'Union européenne

6.2.1 Dans la mesure où les Données personnelles du Client sont transférées d'un Pays européen vers un Pays concerné, HP met à disposition les mécanismes de transfert énumérés ci-dessous qui s'appliqueront, dans l'ordre de priorité indiqué à la clause 6.2.2, à ces transferts conformément aux Lois relatives à la protection de la vie privée et des données personnelles :

6.2.1.1 Règles d'entreprise contraignantes HP pour les Sous-traitants, s'il y a lieu : HP a adopté des règles d'entreprise contraignantes pour les Sous-traitants qui couvrent les Données personnelles du Client qu'elle traite: HP doit maintenir ces règles d'entreprise contraignantes pour les processeurs HP et informer rapidement le client dans le cas où les règles d'entreprise contraignantes pour les processeurs HP ne constituent plus un

mécanisme de transfert valide. Les règles d'entreprise contraignantes pour les processeurs HP sont disponibles sur ce lien : https://www.hp.com/uk-en/bcr-pages.html?jumpid=in_R11928_/us/en/corp/privacy-central/binding-corporate-rules .

6.2.1.2 Mécanisme de conformité approuvé par l'Europe et les États-Unis : Tout transfert dans le cadre d'un mécanisme de conformité approuvé par l'Europe et les États-Unis doit être effectué conformément aux règles du mécanisme, y compris, le cas échéant, l'enregistrement ou la certification de la ou des sociétés affiliées de HP situées aux États-Unis d'Amérique, qui traiteront les Données personnelles du Client aux fins des Services.

6.2.1.3 Clauses contractuelles types de l'UE, soit du Responsable de traitement de données au Sous-traitant des données (pièce jointe 2) soit du Sous-traitant des données au Sous-traitant des données (pièce jointe 3), selon le cas.

6.2.2 Dans le cas où les Services sont couverts par plus d'un mécanisme de transfert, le transfert des Données personnelles du Client sera soumis à un seul mécanisme de transfert conformément à l'ordre de priorité suivant : 1) Règles d'entreprise contraignantes HP pour les Sous-traitants ; 2) Mécanisme de conformité approuvé par l'Europe et les États-Unis ; 3) Les Clauses contractuelles types de l'UE.

6.3 Dispositions spécifiques au Royaume-Uni

6.3.1 Dans la mesure où les Données personnelles du Client sont transférées du Royaume-Uni vers un Pays concerné, le mécanisme de transfert décrit à l'Annexe 4 s'applique.

6.4 Dispositions spécifiques à l'Argentine

6.4.1 Dans la mesure où les Données personnelles du client sont transférées de l'Argentine vers un Pays concerné, le mécanisme de transfert visé à l'Annexe 5 s'applique.

6.5 Dispositions spécifiques à la Chine

6.5.1 Dans la mesure où des Données personnelles du client collectées ou générées en Chine sont transférées de la République populaire de Chine par HP vers un pays ou une région en dehors de la Chine, HP met à disposition le mécanisme de transfert indiqué ci-dessous :

6.5.1.1 Contrat standard (annexe 6) : le Client doit conclure un contrat standard publié par la CAC avec le bénéficiaire des Données personnelles du Client.

6.5.2 Lorsque le Responsable de traitement transfère des Données personnelles depuis la République populaire de Chine vers un Sous-traitant dans un pays ou une région hors de Chine, le Responsable de traitement est responsable de l'obtention du consentement des personnes concernées par le transfert.

6.6 Dispositions spécifiques au Brésil

6.6.1 Dans la mesure où les Données personnelles du Client sont transférées du Brésil vers un Pays concerné, ces transferts ne peuvent avoir lieu que conformément à l'un des mécanismes énumérés ci-dessous, par ordre de priorité :

6.6.1.1 Le cas échéant, Règles d'entreprise contraignantes de HP en tant que sous-traitant : HP a adopté des Règles d'entreprise contraignantes en tant que sous-traitant qui couvrent les Données personnelles du Client qu'elle traite. HP doit maintenir ces Règles d'entreprise contraignantes de HP en tant que sous-traitant et informer rapidement le Client si les Règles d'entreprise contraignantes de HP en tant que sous-traitant ne constituent plus un mécanisme de transfert valide.

6.6.1.2 Clauses contractuelles types pour le Brésil (Annexe 7).

6.7 Dispositions spécifiques à l'Arabie saoudite

6.7.1 Dans la mesure où les Données personnelles du Client sont transférées de l'Arabie saoudite vers un Pays concerné, les mécanismes de transfert mentionnés à l'Annexe 8 (Responsable du traitement des données principal) ou à l'Annexe 9 (Responsable du traitement des données délégué) s'appliquent.

7 AUDITS

7.1 Sur demande écrite du Client, HP mettra à la disposition de celui-ci toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les Lois relatives à la protection de la vie privée et des données personnelles, étant entendu que HP n'est pas tenue de fournir des informations commercialement confidentielles. Une fois par an au maximum et aux frais du Client, HP autorisera et contribuera aux audits par le Client ou son auditeur tiers indépendant autorisé, qui ne sera pas un concurrent de HP. La portée de ces audits, y compris les conditions de confidentialité, sera convenue mutuellement par les Parties avant leur lancement. Pour garantir que le Client a le droit de prendre des mesures appropriées pour arrêter ou corriger toute utilisation non autorisée des Données personnelles du Client par HP, les parties confirmeront et développeront un plan de correction mutuellement approuvé, selon le besoin, pour traiter tout constat de l'audit qui implique une telle utilisation non autorisée des Données personnelles du Client.

Liste des Appendices

Appendice 1

Détails du traitement

HP peut périodiquement mettre à jour la présente Appendice 1 afin de refléter les modifications apportées aux activités de traitement.

Catégories de personnes concernées

- Employés, agents et Sous-traitants du Client.

Types de Données personnelles

Les Données personnelles du Client traitées par HP dans le cadre de sa prestation de Services sont déterminées et contrôlées par le Client en tant que Responsable de traitement et conformément à la description des Services cahier des charges et/ou aux bons de commande applicables, mais peuvent inclure à titre d'exemple :

- *des données de contact ou coordonnées* , telles que le nom, le numéro de téléphone professionnel ou personnel, l'adresse électronique professionnelle ou personnelle et l'adresse postale professionnelle de l'entreprise ;

- *des données d'identification de sécurité*, telles que l'identification de l'employé ou le numéro de son badge ;

- *des données d'utilisation du produit*, telles que les pages imprimées, les types de périphériques à l'origine des travaux d'impression, le mode d'impression, le support utilisé, la marque d'encre ou de toner, le type de fichier imprimé (.pdf, .jpg, etc.), l'application utilisée pour l'impression (Word, Excel, Adobe Photoshop, etc.), la taille du fichier, l'horodatage, ainsi que l'utilisation et l'état des fournitures de l'imprimante ;

- *des données de performance*, c'est-à-dire les événements d'impression, les fonctions et alertes utilisées, telles que les avertissements de « niveau d'encre bas », l'utilisation de cartes photo, la télécopie, la numérisation, le serveur Web intégré et d'autres informations techniques qui varient selon le produit ;

- *des données relatives aux équipements* , c'est-à-dire les informations relatives aux ordinateurs, aux imprimantes et/ou aux périphériques, telles que le système d'exploitation, la capacité de mémoire, la région, la langue, le fuseau horaire, le numéro de modèle, la date de première mise en service, l'âge du périphérique, la date de fabrication du périphérique, la version du navigateur, le fabricant de l'ordinateur, le port de connexion, l'état de la garantie, les identifiants uniques du périphérique, les identifiants publicitaires et d'autres informations techniques qui varient selon le produit ;

- *des données sur l'application*, c'est-à-dire les informations relatives aux applications HP, telles que l'emplacement, la langue, la version des logiciels, les préférences en matière de partage des données et les données de mise à jour ; et

- d'autres Données personnelles fournies par une Personne Concernée lorsqu'elle interagit en personne, en ligne, par téléphone ou par courrier avec des centres de service, des services d'assistance ou d'autres canaux d'assistance clientèle afin de faciliter la prestation des Services HP et de répondre aux demandes du Client et/ou de la Personne Concernée ; ou (ii) sur des équipements reçus par HP.

HP ne traitera pas les Données personnelles des Clients à des fins de publicité, de marketing direct, de profilage ou de recherche pour le compte de tiers, sauf si ce traitement est (i) nécessaire pour se conformer aux instructions du Client, ou (ii) fait partie des produits et services HP demandés par le Client.

Activités de traitement

Les Données personnelles du Client traitées dans le cadre du Contrat de Services seront utilisées par HP pour gérer la relation avec le Client et lui fournir des services. HP peut traiter les Données personnelles du Client pour :

- fournir des services de gestion de parc tels que les services de mise à disposition de l'appareil en tant que service (DaaS) et les services de gestion des impressions (MPS) en tant que service ;

- tenir à jour les données de contact et d'enregistrement afin de fournir des services d'assistance et de maintenance complets, y compris les services de type care-pack et les extensions de garantie, et de faciliter les réparations et les retours ;

- faciliter l'accès aux portails pour la consultation et la gestion des données, la gestion des appareils ou périphériques, la commande et l'exécution de commandes de produits ou de services, dans le but de gérer les comptes et d'organiser les expéditions et les livraisons ;

- améliorer les performances et le fonctionnement des produits, des solutions, des services et de l'assistance, y compris l'assistance pendant la garantie et les mises à jour et alertes logicielles et micrologiciels en temps utile pour assurer le fonctionnement continu de l'appareil ou du service ;

- envoyer des messages opérationnels au Client concernant les Services. Les messages opérationnels peuvent inclure des réponses aux demandes de renseignements ou aux requêtes du Client, des rapports sur l'utilisation ou les performances des produits, des messages relatifs à l'achèvement des services ou à la garantie, des notifications de rappel de sécurité ou des mises à jour d'entreprise applicables liées aux fusions, acquisitions ou cessions ;

- maintenir l'intégrité et la sécurité des sites Web, des produits, des fonctionnalités et des services de HP ainsi que prévenir et détecter les menaces à la sécurité, la fraude ou toute autre activité criminelle ou malveillante susceptible de compromettre les informations du Client ;

- vérifier l'identité du Client, notamment en demandant le nom de l'appelant et son numéro d'identification ou de badge pour la prestation des services de télémaintenance de HP ;

- se conformer aux lois et réglementations applicables, aux ordonnances des tribunaux, aux demandes du gouvernement et des autorités chargées de l'application de la loi, ainsi que pour protéger les employés et les autres clients et pour résoudre les litiges ;

- offrir une expérience sur mesure, personnaliser les Services et les communications et créer des recommandations ; et

- effacer les données des appareils retournés à HP.

Appendice 2

Clauses Contractuelles Types de l'UE (du Responsable de traitement au Sous-traitant)

SECTION I

Clause 1

Finalités et champ d'application

(a) Les présentes clauses contractuelles types visent à garantir le respect des exigences du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) en cas de transfert de données à caractère personnel vers un pays tiers.

(b) Les parties:

(i) la ou les personnes physiques ou morales, la ou les autorités publiques, la ou les agences ou autre(s) organisme(s) (ci-après la ou les «entités») qui transfèrent les données à caractère personnel, mentionnés à l'annexe I.A. (ci-après l'«exportateur de données»), et

(ii) la ou les entités d'un pays tiers qui reçoivent les données à caractère personnel de l'exportateur de données, directement ou indirectement par l'intermédiaire d'une autre entité également partie aux présentes clauses, mentionnées à l'annexe I.A. (ci-après l'«importateur de données»)

sont convenues des présentes clauses contractuelles types (ci-après les «clauses»).

(c) Les présentes clauses s'appliquent au transfert de données à caractère personnel précisé à l'annexe I.B.

(d) L'appendice aux présentes clauses, qui contient les annexes qui y sont mentionnées, fait partie intégrante des présentes clauses.

Clause 2

Effet et invariabilité des clauses

(a) Les présentes clauses établissent des garanties appropriées, notamment des droits opposables pour la personne concernée et des voies de droit effectives, en vertu de l'article 46, paragraphe 1, et de l'article 46, paragraphe 2, point c), du règlement (UE) 2016/679 et, en ce qui concerne les transferts de données de responsables du traitement à sous-traitants et/ou de sous-traitants à sous-traitants, des clauses contractuelles types en vertu de l'article 28, paragraphe 7, du règlement (UE) 2016/679, à condition qu'elles ne soient pas modifiées, sauf pour sélectionner le ou les modules appropriés ou pour ajouter ou mettre à jour des informations dans l'appendice. Cela n'empêche pas les parties d'inclure les clauses contractuelles types prévues dans les présentes clauses dans un contrat plus large et/ou d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les présentes clauses et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

(b) Les présentes clauses sont sans préjudice des obligations auxquelles l'exportateur de données est soumis en vertu du règlement (UE) 2016/679.

Clause 3

Tiers bénéficiaires

(a) Les personnes concernées peuvent invoquer et faire appliquer les présentes clauses, en tant que tiers bénéficiaires, contre l'exportateur et/ou l'importateur de données, avec les exceptions suivantes:

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

(ii) clause 8 - module 1: clause 8.5, paragraphe e), et clause 8.9, paragraphe b); module 2: clause 8.1, paragraphe b), clause 8.9, paragraphes a), c), d) et e); module 3: clause 8.1, paragraphes a), c) et d) et clause 8.9, paragraphes a), c), d), e), f) et g); module 4: clause 8.1, paragraphe b), et clause 8.3, paragraphe b);

(iii) clause 9 - module 2: clause 9, paragraphes a), c), d) et e); module 3: clause 9, paragraphes a) c), d) et e);

(iv) clause 12 - module 1: clause 12, paragraphes a) et d); modules 2 et 3: clause 12, paragraphes a), d) et f);

(v) clause 13;

(vi) clause 15.1, paragraphes c), d) et e);

(vii) clause 16, paragraphe e);

(viii) clause 18 - modules 1, 2 et 3: clause 18, paragraphes a) et b); module 4: clause 18.

(b) Le paragraphe a) est sans préjudice des droits des personnes concernées au titre du règlement (UE) 2016/679.

Clause 4

Interprétation

(a) Lorsque les présentes clauses utilisent des termes définis dans le règlement (UE) 2016/679, ceux-ci ont la même signification que dans ledit règlement.

(b) Les présentes clauses sont lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679.

(c) Les présentes clauses ne sont pas interprétées dans un sens contraire aux droits et obligations prévus dans le règlement (UE) 2016/679.

Clause 5

Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes entre les parties existant au moment où les présentes clauses sont convenues, ou souscrites par la suite, les présentes clauses prévalent.

Clause 6

Description du ou des transferts

Les détails du ou des transferts, en particulier les catégories de données à caractère personnel qui sont transférées et la ou les finalités pour lesquelles elles le sont, sont précisés à l'annexe I.B.

Clause 7 - Facultative

Clause d'adhésion

(a) Une entité qui n'est pas partie aux présentes clauses peut, avec l'accord des parties, y adhérer à tout moment, soit en tant qu'exportateur de données soit en tant qu'importateur de données, en remplissant l'appendice et en signant l'annexe I.A.

(b) Une fois l'appendice rempli et l'annexe I.A. signée, l'entité adhérente devient partie aux présentes clauses et a les droits et obligations d'un exportateur de données ou d'un importateur de données selon sa désignation dans l'annexe I.A.

(c) L'entité adhérente n'a aucun droit ni obligation découlant des présentes clauses pour la période antérieure à son adhésion à celles-ci.

SECTION II – OBLIGATIONS DES PARTIES

Clause 8

Garanties en matière de protection des données

L'exportateur de données garantit qu'il a entrepris des démarches raisonnables pour s'assurer que l'importateur de données est à même, par la mise en œuvre de mesures techniques et organisationnelles appropriées, de satisfaire aux obligations qui lui incombent en vertu des présentes clauses.

8.1 Instructions

(a) L'importateur de données ne traite les données à caractère personnel que sur instructions documentées de l'exportateur de données. L'exportateur de données peut donner ces instructions pendant toute la durée du contrat.

(b) S'il n'est pas en mesure de suivre ces instructions, l'importateur de données en informe immédiatement l'exportateur de données.

8.2 Limitation des finalités

L'importateur de données traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du transfert, telles que précisées à l'annexe I.B, sauf en cas d'instructions supplémentaires de l'exportateur de données.

8.3 Transparence

Sur demande, l'exportateur de données met gratuitement à la disposition de la personne concernée une copie des présentes clauses, notamment de l'appendice tel que rempli par les parties. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les mesures décrites à l'annexe II et les données à caractère personnel, l'exportateur de données peut occulter une partie du texte de l'appendice aux présentes clauses avant d'en communiquer une copie, mais fournit un résumé valable s'il serait autrement impossible, pour la personne concernée, d'en comprendre le contenu ou d'exercer ses droits. Les parties fournissent à la personne concernée, à la demande de celle-ci, les motifs des occultations, dans la mesure du possible sans révéler les informations occultées. Cette clause est sans préjudice des obligations qui incombent à l'exportateur de données en vertu des articles 13 et 14 du règlement (UE) 2016/679.

8.4 Exactitude

Si l'importateur de données se rend compte que les données à caractère personnel qu'il a reçues sont inexactes, ou sont obsolètes, il en informe l'exportateur de données dans les meilleurs délais. Dans ce cas, l'importateur de données coopère avec l'exportateur de données pour effacer ou rectifier les données.

8.5 Durée du traitement et effacement ou restitution des données

Le traitement par l'importateur de données n'a lieu que pendant la durée précisée à l'annexe I.B. Au terme de la prestation des services de traitement, l'importateur de données, à la convenance de l'exportateur de données, efface toutes les données à caractère personnel traitées pour le compte de ce dernier et lui en apporte la preuve, ou lui restitue toutes les données à caractère personnel traitées pour son compte et efface les copies existantes. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données à caractère personnel que dans la mesure où et aussi longtemps que cette législation locale l'exige. Ceci est sans préjudice de la clause 14, en particulier de l'obligation imposée à l'importateur de données par la clause 14, paragraphe e), d'informer l'exportateur de données, pendant toute la durée du contrat, s'il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences de la clause 14, paragraphe a).

8.6 Sécurité du traitement

(a) L'importateur de données et, durant la transmission, l'exportateur de données mettent en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données, notamment pour les protéger d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à ces données (ci-après la «violation de données à caractère personnel»). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et de la ou des finalités du traitement ainsi que des risques inhérents au traitement pour les personnes concernées. Les parties envisagent en particulier de recourir au chiffrement ou à la pseudonymisation, notamment pendant la transmission, lorsque la finalité du traitement peut être atteinte de cette manière. En cas de pseudonymisation, les

informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée précise restent, dans la mesure du possible, sous le contrôle exclusif de l'exportateur de données. Pour s'acquitter des obligations qui lui incombent en vertu du présent paragraphe, l'importateur de données met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe II. Il procède à des contrôles réguliers pour s'assurer que ces mesures continuent d'offrir le niveau de sécurité approprié.

(b) L'importateur de données ne donne l'accès aux données à caractère personnel aux membres de son personnel que dans la mesure strictement nécessaire à la mise en œuvre, à la gestion et au suivi du contrat. Il veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

(c) En cas de violation de données à caractère personnel concernant des données à caractère personnel traitées par l'importateur de données au titre des présentes clauses, ce dernier prend des mesures appropriées pour remédier à la violation, y compris des mesures visant à en atténuer les effets négatifs. L'importateur de données informe également l'exportateur de données de cette violation dans les meilleurs délais après en avoir eu connaissance. Cette notification contient les coordonnées d'un point de contact auprès duquel il est possible d'obtenir plus d'informations, ainsi qu'une description de la nature de la violation (y compris, si possible, les catégories et le nombre approximatif de personnes concernées et d'enregistrements de données à caractère personnel concernés), de ses conséquences probables et des mesures prises ou proposées pour y remédier, y compris, le cas échéant, des mesures visant à en atténuer les effets négatifs potentiels. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et les autres informations sont fournies par la suite, dans les meilleurs délais, à mesure qu'elles deviennent disponibles.

(d) L'importateur de données coopère avec l'exportateur de données et l'aide afin de lui permettre de respecter les obligations qui lui incombent en vertu du règlement (UE) 2016/679, notamment celle d'informer l'autorité de contrôle compétente et les personnes concernées, compte tenu de la nature du traitement et des informations à la disposition de l'importateur de données.

8.7 Données sensibles

Lorsque le transfert concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne, ou des données relatives à des condamnations pénales et à des infractions (ci-après les «données sensibles»), l'importateur de données applique les restrictions particulières et/ou les garanties supplémentaires décrites à l'annexe I.B.

8.8 Transferts ultérieurs

L'importateur de données ne divulgue les données à caractère personnel à un tiers que sur instructions documentées de l'exportateur de données. En outre, les données ne peuvent être divulguées à un tiers situé en dehors de l'Union européenne (dans le même pays que l'importateur de données ou dans un autre pays tiers, ci-après «transfert ultérieur»), que si le tiers est lié par les présentes clauses ou accepte de l'être, en vertu du module approprié, ou si:

(i) le transfert ultérieur est effectué vers un pays bénéficiant d'une décision d'adéquation en vertu de l'article 45 du règlement (UE) 2016/679 qui couvre le transfert ultérieur;

(ii) le tiers offre d'une autre manière des garanties appropriées conformément aux articles 46 ou 47 du règlement (UE) 2016/679 en ce qui concerne le traitement en question;

(iii) le transfert ultérieur est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dans le contexte de procédures administratives, réglementaires ou judiciaires spécifiques; ou

(iv) le transfert ultérieur est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Tout transfert ultérieur est soumis au respect, par l'importateur de données, de toutes les autres garanties au titre des présentes clauses, en particulier de la limitation des finalités.

8.9 Documentation et conformité

(a) L'importateur de données traite rapidement et de manière appropriée les demandes de renseignements de l'exportateur de données concernant le traitement au titre des présentes clauses.

(b) Les parties sont en mesure de démontrer le respect des présentes clauses. En particulier, l'importateur de données conserve une trace documentaire appropriée des activités de traitement menées pour le compte de l'exportateur de données.

(c) L'importateur de données met à la disposition de l'exportateur de données toutes les informations nécessaires pour démontrer le respect des obligations prévues par les présentes clauses et, à la demande de l'exportateur de données, pour permettre la réalisation d'audits des activités de traitement couvertes par les présentes clauses, et contribuer à ces audits, à intervalles raisonnables ou s'il existe des indications de non-respect. Lorsqu'il décide d'un examen ou d'un audit, l'exportateur de données peut tenir compte des certifications pertinentes détenues par l'importateur de données.

(d) L'exportateur de données peut choisir de procéder à l'audit lui-même ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques de l'importateur de données et sont, le cas échéant, effectués avec un préavis raisonnable.

(e) Les parties mettent à la disposition de l'autorité de contrôle compétente, à la demande de celle-ci, les informations mentionnées aux paragraphes b) et c), y compris les résultats de tout audit.

Clause 9

Recours à des sous-traitants ultérieurs

(a) L'importateur de données a l'autorisation générale de l'exportateur de données de recruter un ou plusieurs sous-traitants ultérieurs à partir d'une liste arrêtée d'un commun accord. L'importateur de données informe expressément par écrit l'exportateur de données de tout changement concernant l'ajout ou le remplacement de sous-traitants ultérieurs qu'il est prévu d'apporter à cette liste au moins [*précisez le délai*] à l'avance, donnant ainsi à l'exportateur de données suffisamment de temps pour émettre des objections à l'encontre de ces changements avant le recrutement du ou des sous-traitants ultérieurs L'importateur de données fournit à l'exportateur de données les informations nécessaires pour permettre à ce dernier d'exercer son droit d'émettre des objections.

(b) Lorsque l'importateur de données recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte de l'exportateur de données), il le fait au moyen d'un contrat écrit qui prévoit, en substance, les mêmes obligations en matière de protection des données que

celles qui lient l'importateur de données au titre des présentes clauses, notamment en ce qui concerne les droits du tiers bénéficiaire pour les personnes concernées. Les parties conviennent qu'en respectant la présente clause, l'importateur de données satisfait aux obligations qui lui incombent en vertu de la clause 8.8. L'importateur de données veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses.

(c) L'importateur de données fournit à l'exportateur de données, à la demande de celui-ci, une copie du contrat avec le sous-traitant ultérieur et de ses éventuelles modifications ultérieures. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les données à caractère personnel, l'importateur de données peut occulter une partie du texte du contrat avant d'en communiquer une copie.

(d) L'importateur de données reste pleinement responsable à l'égard de l'exportateur de données de l'exécution des obligations qui incombent au sous-traitant ultérieur en vertu du contrat qu'il a conclu avec lui. L'importateur de données notifie à l'exportateur de données tout manquement du sous-traitant ultérieur aux obligations qui lui incombent en vertu dudit contrat.

(e) L'importateur de données convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire en vertu de laquelle, dans les cas où l'importateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'exportateur de données a le droit de résilier le contrat du sous-traitant ultérieur et de donner instruction à ce dernier d'effacer ou de restituer les données à caractère personnel.

Clause 10

Droits des personnes concernées

(a) L'importateur de données informe rapidement l'exportateur de données de toute demande reçue d'une personne concernée. Il ne répond pas lui-même à cette demande, à moins d'y avoir été autorisé par l'exportateur de données.

(b) L'importateur de données aide l'exportateur de données à s'acquitter de son obligation de répondre aux demandes de personnes concernées désireuses d'exercer leurs droits en vertu du règlement (UE) 2016/679. À cet égard, les parties indiquent à l'annexe II les mesures techniques et organisationnelles appropriées, compte tenu de la nature du traitement, au moyen desquelles l'aide sera fournie, ainsi que la portée et l'étendue de l'aide requise.

(c) Lorsqu'il s'acquitte des obligations qui lui incombent en vertu des paragraphes a) et b), l'importateur de données se conforme aux instructions de l'exportateur de données.

Clause 11

Voies de recours

(a) L'importateur de données informe les personnes concernées, sous une forme transparente et aisément accessible, au moyen d'une notification individuelle ou sur son site web, d'un point de contact autorisé à traiter les réclamations. Il traite sans délai toute réclamation reçue d'une personne concernée.

(b) En cas de litige entre une personne concernée et l'une des parties portant sur le respect des présentes clauses, cette partie met tout en œuvre pour parvenir à un règlement à l'amiable dans les meilleurs délais. Les parties se tiennent mutuellement informées de ces litiges et, s'il y a lieu, coopèrent pour les résoudre.

(c) Lorsque la personne concernée invoque un droit du tiers bénéficiaire en vertu de la clause 3, l'importateur de données accepte la décision de la personne concernée:

(i) d'introduire une réclamation auprès de l'autorité de contrôle de l'État membre dans lequel se trouve sa résidence habituelle ou son lieu de travail, ou auprès de l'autorité de contrôle compétente au sens de la clause 13;

(ii) de renvoyer le litige devant les juridictions compétentes au sens de la clause 18.

(d) Les parties acceptent que la personne concernée puisse être représentée par un organisme, une organisation ou une association à but non lucratif dans les conditions énoncées à l'article 80, paragraphe 1, du règlement (UE) 2016/679.

(e) L'importateur de données se conforme à une décision qui est contraignante en vertu du droit applicable de l'Union ou d'un État membre.

(f) L'importateur de données convient que le choix effectué par la personne concernée ne remettra pas en cause le droit procédural et matériel de cette dernière d'obtenir réparation conformément à la législation applicable.

Clause 12

Responsabilité

(a) Chaque partie est responsable envers la ou les autres parties des dommages qu'elle cause à l'autre ou aux autres parties du fait d'un manquement aux présentes clauses.

(b) L'importateur de données est responsable à l'égard de la personne concernée, et la personne concernée a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par l'importateur de données ou son sous-traitant ultérieur du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses.

(c) Nonobstant le paragraphe b), l'exportateur de données est responsable à l'égard de la personne concernée et celle-ci a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par l'exportateur de données ou l'importateur de données (ou son sous-traitant ultérieur) du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses. Ceci est sans préjudice de la responsabilité de l'exportateur de données et, si l'exportateur de données est un sous-traitant agissant pour le compte d'un responsable du traitement, de la responsabilité de ce dernier au titre du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725, selon le cas.

(d) Les parties conviennent que, si l'exportateur de données est reconnu responsable, en vertu du paragraphe c), du dommage causé par l'importateur de données (ou son sous-traitant ultérieur), il a le droit de réclamer auprès de l'importateur de données la part de la réparation correspondant à la responsabilité de celui-ci dans le dommage.

(e) Lorsque plusieurs parties sont responsables d'un dommage causé à la personne concernée du fait d'une violation des présentes clauses, toutes les parties responsables le sont conjointement et solidairement et la personne concernée a le droit d'intenter une action en justice contre n'importe laquelle de ces parties.

(f) Les parties conviennent que, si la responsabilité d'une d'entre elles est reconnue en vertu du paragraphe e), celle-ci a le droit de réclamer auprès de l'autre ou des autres parties la part de la réparation correspondant à sa/leur responsabilité dans le dommage.

(g) L'importateur de données ne peut invoquer le comportement d'un sous-traitant ultérieur pour échapper à sa propre responsabilité.

Clause 13

Contrôle

(a) [Si l'exportateur de données est établi dans un État membre de l'Union:] L'autorité de contrôle chargée de garantir le respect, par l'exportateur de données, du règlement (UE) 2016/679 en ce qui concerne le transfert de données, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité de contrôle compétente.

[Si l'exportateur de données n'est pas établi dans un État membre de l'Union, mais relève du champ d'application territorial du règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2, et a désigné un représentant en vertu de l'article 27, paragraphe 1, dudit règlement:] L'autorité de contrôle de l'État membre dans lequel le représentant au sens de l'article 27, paragraphe 1, du règlement (UE) 2016/679 est établi, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité de contrôle compétente.

[Si l'exportateur de données n'est pas établi dans un État membre de l'Union, mais relève du champ d'application territorial du règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2 sans toutefois avoir à désigner un représentant en vertu de l'article 27, paragraphe 2, du règlement (UE) 2016/679:] L'autorité de contrôle d'un des États membres dans lesquels se trouvent les personnes concernées dont les données à caractère personnel sont transférées au titre des présentes clauses en lien avec l'offre de biens ou de services ou dont le comportement fait l'objet d'un suivi, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité compétente.

(b) L'importateur de données accepte de se soumettre à la juridiction de l'autorité de contrôle compétente et de coopérer avec elle dans le cadre de toute procédure visant à garantir le respect des présentes clauses. En particulier, l'importateur de données accepte de répondre aux demandes de renseignements, de se soumettre à des audits et de se conformer aux mesures adoptées par l'autorité de contrôle, notamment aux mesures correctrices et compensatoires. Il confirme par écrit à l'autorité de contrôle que les mesures nécessaires ont été prises.

SECTION III – LÉGISLATIONS LOCALES ET OBLIGATIONS EN CAS D'ACCÈS DES AUTORITÉS PUBLIQUES

Clause 14

Législations et pratiques locales ayant une incidence sur le respect des clauses

(a) Les parties garantissent qu'elles n'ont aucune raison de croire que la législation et les pratiques du pays tiers de destination applicables au traitement des données à caractère personnel par l'importateur de données, notamment les exigences en matière de divulgation de données à caractère personnel ou les mesures autorisant l'accès des autorités publiques à ces données, empêchent l'importateur de données de s'acquitter des obligations qui lui incombent en vertu des présentes clauses. Cette disposition repose sur l'idée que les législations et les pratiques qui respectent l'essence des libertés et droits fondamentaux et qui n'excèdent pas ce qui est nécessaire et proportionné dans une société démocratique pour préserver un des objectifs énumérés à l'article 23, paragraphe 1, du règlement (UE) 2016/679 ne sont pas en contradiction avec les présentes clauses.

(b) Les parties déclarent qu'en fournissant la garantie mentionnée au paragraphe a), elles ont dûment tenu compte, en particulier, des éléments suivants:

(i) des circonstances particulières du transfert, parmi lesquelles la longueur de la chaîne de traitement, le nombre d'acteurs concernés et les canaux de transmission utilisés; les transferts ultérieurs prévus; le type de destinataire; la finalité du traitement; les catégories et le format des données à caractère personnel transférées; le secteur économique dans lequel le transfert a lieu et le lieu de stockage des données transférées;

(ii) des législations et des pratiques du pays tiers de destination – notamment celles qui exigent la divulgation de données aux autorités publiques ou qui autorisent l'accès de ces dernières aux données – pertinentes au regard des circonstances particulières du transfert, ainsi que des limitations et des garanties applicables[1];

(iii) de toute garantie contractuelle, technique ou organisationnelle pertinente mise en place pour compléter les garanties prévues par les présentes clauses, y compris les mesures appliquées pendant la transmission et au traitement des données à caractère personnel dans le pays de destination.

(c) L'importateur de données garantit que, lors de l'évaluation au titre du paragraphe b), il a déployé tous les efforts possibles pour fournir des informations pertinentes à l'exportateur de données et convient qu'il continuera à coopérer avec ce dernier pour garantir le respect des présentes clauses.

(d) Les parties conviennent de conserver une trace documentaire de l'évaluation au titre du paragraphe b) et de mettre cette évaluation à la disposition de l'autorité de contrôle compétente si celle-ci en fait la demande.

(e) L'importateur de données accepte d'informer sans délai l'exportateur de données si, après avoir souscrit aux présentes clauses et pendant la durée du contrat, il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences du paragraphe a), notamment à la suite d'une modification de la législation du pays tiers ou d'une mesure (telle qu'une demande de divulgation) indiquant une application pratique de cette législation qui n'est pas conforme aux exigences du paragraphe a).

(f) À la suite d'une notification au titre du paragraphe e), ou si l'exportateur de données a d'autres raisons de croire que l'importateur de données ne peut plus s'acquitter des obligations qui lui incombent en vertu des présentes clauses, l'exportateur de données définit sans délai les mesures appropriées (par exemple des mesures techniques ou organisationnelles visant à garantir la sécurité et la confidentialité) qu'il doit adopter et/ou qui doivent être adoptées par l'importateur de données pour remédier à la situation. L'exportateur de données suspend le transfert de données s'il estime qu'aucune garantie appropriée ne peut être fournie pour ce transfert ou si l'autorité de contrôle compétente lui en donne l'instruction. Dans ce cas, l'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient

1 En ce qui concerne l'incidence de ces législations et pratiques sur le respect des présentes clauses, différents éléments peuvent être considérés comme faisant partie d'une évaluation globale. Ces éléments peuvent inclure une expérience concrète, documentée et pertinente de cas antérieurs de demandes de divulgation émanant d'autorités publiques, ou l'absence de telles demandes, couvrant un laps de temps suffisamment représentatif. Il peut s'agir de registres internes ou d'autres documents établis de manière continue conformément au principe de diligence raisonnable et certifiés à un niveau hiérarchique élevé, pour autant que ces informations puissent être partagées légalement avec des tiers. Lorsque cette expérience pratique est invoquée pour conclure que l'importateur de données ne sera pas empêché de respecter les présentes clauses, il y a lieu de l'étayer par d'autres éléments pertinents et objectifs, et il appartient aux parties d'examiner avec soin si ces éléments, pris dans leur ensemble, ont un poids suffisant, du point de vue de leur fiabilité et de leur représentativité, pour soutenir cette conclusion. En particulier, les parties doivent s'assurer que leur expérience pratique est corroborée et non contredite par des informations fiables accessibles au public ou disponibles d'une autre manière sur l'existence ou l'absence de demandes dans le même secteur et/ou sur l'application pratique du droit, comme la jurisprudence et les rapports d'organes de contrôle indépendants.

convenues autrement. Lorsque le contrat est résilié en vertu de la présente clause, la clause 16, paragraphes d) et e), s'applique.

Clause 15

Obligations de l'importateur de données en cas d'accès des autorités publiques

15.1 Notification

(a) L'importateur de données convient d'informer sans délai l'exportateur de données et, si possible, la personne concernée (si nécessaire avec l'aide de l'exportateur de données):

(i) s'il reçoit une demande juridiquement contraignante d'une autorité publique, y compris judiciaire, en vertu de la législation du pays de destination en vue de la divulgation de données à caractère personnel transférées au titre des présentes clauses; cette notification comprend des informations sur les données à caractère personnel demandées, l'autorité requérante, la base juridique de la demande et la réponse fournie; ou

(ii) s'il a connaissance d'un quelconque accès direct des autorités publiques aux données à caractère personnel transférées au titre des présentes clauses en vertu de la législation du pays de destination; cette notification comprend toutes les informations dont l'importateur de données dispose.

(b) Si la législation du pays de destination interdit à l'importateur de données d'informer l'exportateur de données et/ou la personne concernée, l'importateur de données convient de tout mettre en œuvre pour obtenir une levée de cette interdiction, en vue de communiquer autant d'informations que possible, dans les meilleurs délais. L'importateur de données accepte de garder une trace documentaire des efforts qu'il a déployés afin de pouvoir en apporter la preuve à l'exportateur de données, si celui-ci lui en fait la demande.

(c) Lorsque la législation du pays de destination le permet, l'importateur de données accepte de fournir à l'exportateur de données, à intervalles réguliers pendant la durée du contrat, autant d'informations utiles que possible sur les demandes reçues (notamment le nombre de demandes, le type de données demandées, la ou les autorités requérantes, la contestation ou non des demandes et l'issue de ces contestations, etc.).

(d) L'importateur de données accepte de conserver les informations mentionnées aux paragraphes a) à c) pendant la durée du contrat et de les mettre à la disposition de l'autorité de contrôle compétente si celle-ci lui en fait la demande.

(e) Les paragraphes a) à c) sont sans préjudice de l'obligation incombant à l'importateur de données, en vertu de la clause 14, paragraphe e), et de la clause 16, d'informer sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses.

15.2 Contrôle de la légalité et minimisation des données

(a) L'importateur de données accepte de contrôler la légalité de la demande de divulgation, en particulier de vérifier si elle s'inscrit dans les limites des pouvoirs conférés à l'autorité publique requérante, et de la contester si, après une évaluation minutieuse, il conclut qu'il existe des motifs raisonnables de considérer qu'elle est illégale en vertu de la législation du pays de destination, des obligations applicables en vertu du droit international et des principes de courtoisie internationale. L'importateur de données exerce les possibilités d'appel ultérieures dans les mêmes conditions. Lorsqu'il conteste une demande, l'importateur de données demande des mesures provisoires visant

à suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente se prononce sur son bien-fondé. Il ne divulgue pas les données à caractère personnel demandées tant qu'il n'est pas obligé de le faire en vertu des règles de procédure applicables. Ces exigences sont sans préjudice des obligations incombant à l'importateur de données en vertu de la clause 14, paragraphe e).

(b) L'importateur de données accepte de garder une trace documentaire de son évaluation juridique ainsi que de toute contestation de la demande de divulgation et, dans la mesure où la législation du pays de destination le permet, de mettre les documents concernés à la disposition de l'exportateur de données. Il les met également à la disposition de l'autorité de contrôle compétente si celle-ci lui en fait la demande.

(c) L'importateur de données accepte de fournir le minimum d'informations autorisé lorsqu'il répond à une demande de divulgation, sur la base d'une interprétation raisonnable de la demande.

SECTION IV — DISPOSITIONS FINALES

Clause 16

Non-respect des clauses et résiliation

(a) L'importateur de données informe sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses, quelle qu'en soit la raison.

(b) Dans le cas où l'importateur de données enfreint les présentes clauses ou n'est pas en mesure de les respecter, l'exportateur de données suspend le transfert de données à caractère personnel à l'importateur de données jusqu'à ce que le respect des présentes clauses soit à nouveau garanti ou que le contrat soit résilié. Ceci est sans préjudice de la clause 14, paragraphe f).

(c) L'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses, lorsque:

(i) l'exportateur de données a suspendu le transfert de données à caractère personnel à l'importateur de données en vertu du paragraphe b) et que le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension;

(ii) l'importateur de données enfreint gravement ou de manière persistante les présentes clauses; ou

(iii) l'importateur de données ne se conforme pas à une décision contraignante d'une juridiction ou d'une autorité de contrôle compétente concernant les obligations qui lui incombent au titre des présentes clauses.

Dans ces cas, il informe l'autorité de contrôle compétente de ce non-respect. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement.

(d) Les données à caractère personnel qui ont été transférées avant la résiliation du contrat au titre du paragraphe c) sont immédiatement restituées à l'exportateur de données ou effacées dans leur intégralité, à la convenance de celui-ci. Il en va de même pour toute copie des données. L'importateur de données apporte la preuve de l'effacement des données à l'exportateur de données. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel transférées, ce dernier

garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données que dans la mesure où et aussi longtemps que cette législation locale l'exige.

(e) Chaque partie peut révoquer son consentement à être liée par les présentes clauses i) si la Commission européenne adopte une décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 qui couvre le transfert de données à caractère personnel auquel les présentes clauses s'appliquent; ou ii) si le règlement (UE) 2016/679 est intégré dans le cadre juridique du pays vers lequel les données à caractère personnel sont transférées. Ceci est sans préjudice des autres obligations qui s'appliquent au traitement en question en vertu du règlement (UE) 2016/679.

Clause 17

Droit applicable

[OPTION 1: Les présentes clauses sont régies par le droit d'un des États membres de l'Union européenne, pour autant que ce droit reconnaisse des droits au tiers bénéficiaire. Les parties conviennent qu'il s'agit du droit de la France

Clause 18

Élection de for et juridiction

(a) Tout litige survenant du fait des présentes clauses est tranché par les juridictions d'un État membre de l'Union européenne.

(b) Les parties conviennent qu'il s'agit des juridictions de la France.

(c) La personne concernée peut également poursuivre l'exportateur et/ou l'importateur de données devant les juridictions de l'État membre dans lequel elle a sa résidence habituelle.

(d) Les parties acceptent de se soumettre à la compétence de ces juridictions.

APPENDICE

ANNEXE I

A. LISTE DES PARTIES

Exportateur(s) de données: [*Identité et coordonnées du ou des exportateurs de données et, le cas échéant, de leur délégué à la protection des données et/ou de leur représentant dans l'Union européenne*]

1. Nom: …

Adresse: …

Nom, fonction et coordonnées de la personne de contact: …

Activités en rapport avec les données transférées au titre des présentes clauses: …

Signature et date: …

Rôle (responsable du traitement/sous-traitant): …

2. …

Importateur(s) de données: [*Identité et coordonnées du ou des importateurs de données, y compris de toute personne de contact chargée de la protection des données*]

1. Nom: …

Adresse: …

Nom, fonction et coordonnées de la personne de contact: …

Activités en rapport avec les données transférées au titre des présentes clauses: …

Signature et date: …

Rôle (responsable du traitement/sous-traitant): …

2. …

B. DESCRIPTION DU TRANSFERT

Catégories de personnes concernées dont les données à caractère personnel sont transférées

……

Catégories de données à caractère personnel transférées

……

Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, telles que la limitation stricte des finalités, les restrictions d'accès (notamment l'accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.

……

Fréquence du transfert (indiquez, par exemple, si les données sont transférées sur une base ponctuelle ou continue).

……

Nature du traitement

……

Finalité(s) du transfert et du traitement ultérieur des données

……

Durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, critères utilisés pour déterminer cette durée

……

Pour les transferts à des sous-traitants (ultérieurs), veuillez également préciser l'objet, la nature et la durée du traitement

……

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

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

ANNEXE II

MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS LES MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À GARANTIR LA SÉCURITÉ DES DONNÉES

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's Information Security program is designed to direct and maintain the organization's information security strategy and controls. This system ensures enterprise-wide compliance with HP's security policies and controls, as well as adherence to the security requirements of its customers. Structured in alignment with industry-standard cybersecurity frameworks, laws, and regulations, the Framework is reviewed annually to adapt to HP's evolving thread landscape.

3. Cybersecurity Risk Management

HP's cybersecurity risk management program is designed to preserve the confidentiality, integrity, and availability of its information assets. The program provides a consistent approach to identifying, assessing, prioritizing, treating, remedying, tracking, and reporting cybersecurity risks. HP defines its Risk Appetite as the acceptable level of loss exposure and Risk Tolerance as the degree of variance from this appetite. Risks are evaluated using a defined methodology, enabling HP to mitigate information security risks to an acceptable level. This program aligns with HP's Enterprise Risk Management process.

4. HR Security

HP Human Resource Security policy ensures information security throughout the employee lifecycle by establishing processes for access to facilities, information systems, and other assets. This includes obtaining written acknowledgments through confidentiality and non-disclosure agreements, as well as conducting background screening procedures. All candidates for employment with HP must complete a background verification check in accordance with relevant laws, regulations, and ethics.

5. Asset Management

HP has a process for identifying technical information assets, categorizing critical assets, and maintaining documented handling procedures for each information classification type, including those containing Personal Data. These procedures cover storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification. HP security policies and standards also mandate the secure disposal of media.

6. Data Security

HP's Data Security program outlines the security practices and technical controls that must be implemented to protect the confidentiality, authenticity, and integrity of data. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification are a few of the factors that determine how information is classified under HP's Data Security policy. In addition to data handling procedures, the policy outlines data encryption, deletion, collection and processing, retention, backup, and data loss prevention.

7. Access Control

HP employs the principle of least privilege for logical access control, providing user access through unique user IDs and passwords. The password policy defines complexity, strength, validity, and password-history controls. Access rights are periodically reviewed and revoked upon personnel departure. Agreed-upon procedures for user account creation and deletion are implemented to grant and revoke access to client systems during engagements.

8. 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. Our Cryptography program involves the use of mathematical techniques to secure information and communications, ensuring that only authorized parties can access the data. A critical component of HP's information security program is protecting data from unauthorized access and tampering.

9. Physical and Environmental Security

HP facilities are secured using various physical and electronic access controls, including security guards, electronic access control, and closed-circuit television (CCTV). Facilities are also equipped with necessary infrastructure support, including temperature control and power backups, using UPS and/or diesel generators to support critical services. All HP personnel are registered and required to carry appropriate identification badges.

10. Operations Management

HP has established minimum hardening requirements for technology infrastructure, including workstations, servers, and network equipment. These devices use pre-hardened operating system images, with requirements varying by operating system and implemented controls. Additionally, HP has deployed Network Intrusion Detection/Prevention Systems (NIDS/NIPS) that are monitored and managed 24/7.

11. Communications Security

Communications Security ensures the protection of information within corporate networks. This includes the installation and management of network security components (e.g., firewalls), segregation of networks, as well as web filtering and email handling controls. Additionally, it involves monitoring and managing communication channels to detect and prevent unauthorized access or data breaches.

12. Systems Security

HP's policy mandates a secure development methodology for systems and software throughout their lifecycle. The Software Development Lifecycle covers initiation, development/acquisition, implementation, operations, and disposal. All system components are evaluated for their impact on overall security. HP has established controls for application service transactions, including user credential validation, digital signatures, encryption, secure communication protocols, and storing transaction details within the appropriate network security zone. Regular internal vulnerability scans are also performed.

13. Third Parties and Subcontractors

HP has processes in place to select sub-contractors who comply with comprehensive contractual security requirements. For applicable suppliers handling HP or customer data, or accessing the HP network, HP Cybersecurity conducts a risk assessment to verify an information security program with physical, technical, and administrative safeguards. This assessment is required before the supplier can access HP information.

14. Information Security Incident Management

HP has a comprehensive Cyber Incident Management Process that outlines purpose, scope, roles, responsibilities, management commitment, organizational coordination, implementation procedures, and compliance checking. This process is reviewed and updated annually. The Cyber Incident Response Team, including HP Cybersecurity personnel trained in incident response and crisis management, conducts regular tabletop reviews of the process and any incidents or events.

15. Business Continuity Management

HP's global Continuity of Operations program ensures end-to-end continuity through collaborative, standardized, and documented planning processes. The company periodically exercises its business continuity plans to ensure effectiveness, testing and updating all plans at least yearly. Additionally, all personnel involved in the business continuity plan receive proper training.

16. Compliance

Compliance shapes HP's approach to meeting legal, contractual, and internal expectations for an effective information security program. Regular information security reviews ensure protocols are integrated into each business group's operations. The review process also keeps documents updated to reflect current legal obligations as requirements evolve.

17. Payment Card Industry

The Payment Card Industry (PCI) framework guides HP's approach to achieving PCI Compliance, outlining business responsibilities and security controls aligned with PCI DSS. By installing and maintaining network security controls like firewalls, HP ensures it meets PCI Compliance requirements.

18. HP Product Security

HP Product Security encompasses essential practices to secure HP Products, such as code signing, managing product security vulnerabilities, issuing security bulletins, and reporting product security issues. These measures ensure that HP products remain secure and reliable for users. Product security is of paramount importance at HP, as it helps maintain customer trust and protects against potential threats.

19. HP Service Security

HP Service Security encompasses essential practices to secure the services provided to HP customers. This policy addresses various areas of service security, including HP infrastructure hosted, third-party hosted, partner hosted, and customer hosted environments. These measures ensure that HP services remain secure and reliable for users. By implementing robust security practices, HP ensures the safety and integrity of its products and services, fostering a secure and trustworthy environment for all users.

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.

Appendice 3

Clauses Contractuelles Types de l'UE (du Sous-traitant à Sous-traitant)

SECTION I

Clause 1
Finalités et champ d'application

(a) Les présentes clauses contractuelles types visent à garantir le respect des exigences du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) en cas de transfert de données à caractère personnel vers un pays tiers.

(b) Les parties:

(i) la ou les personnes physiques ou morales, la ou les autorités publiques, la ou les agences ou autre(s) organisme(s) (ci-après la ou les «entités») qui transfèrent les données à caractère personnel, mentionnés à l'annexe I.A. (ci-après l'«exportateur de données»), et

(ii) la ou les entités d'un pays tiers qui reçoivent les données à caractère personnel de l'exportateur de données, directement ou indirectement par l'intermédiaire d'une autre entité également partie aux présentes clauses, mentionnées à l'annexe I.A. (ci-après l'«importateur de données»)

sont convenues des présentes clauses contractuelles types (ci-après les «clauses»).

(c) Les présentes clauses s'appliquent au transfert de données à caractère personnel précisé à l'annexe I.B.

(d) L'appendice aux présentes clauses, qui contient les annexes qui y sont mentionnées, fait partie intégrante des présentes clauses.

Clause 2
Effet et invariabilité des clauses

(a) Les présentes clauses établissent des garanties appropriées, notamment des droits opposables pour la personne concernée et des voies de droit effectives, en vertu de l'article 46, paragraphe 1, et de l'article 46, paragraphe 2, point c), du règlement (UE) 2016/679 et, en ce qui concerne les transferts de données de responsables du traitement à sous-traitants et/ou de sous-traitants à sous-traitants, des clauses contractuelles types en vertu de l'article 28, paragraphe 7, du règlement (UE) 2016/679, à condition qu'elles ne soient pas modifiées, sauf pour sélectionner le ou les modules appropriés ou pour ajouter ou mettre à jour des informations dans l'appendice. Cela n'empêche pas les parties d'inclure les clauses contractuelles types prévues dans les présentes clauses dans un contrat plus large et/ou d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les présentes clauses et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

(b) Les présentes clauses sont sans préjudice des obligations auxquelles l'exportateur de données est soumis en vertu du règlement (UE) 2016/679.

Clause 3
Tiers bénéficiaires

(a) Les personnes concernées peuvent invoquer et faire appliquer les présentes clauses, en tant que tiers

bénéficiaires, contre l'exportateur et/ou l'importateur de données, avec les exceptions suivantes:

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

(ii) clause 8 - module 1: clause 8.5, paragraphe e), et clause 8.9, paragraphe b); module 2: clause 8.1, paragraphe b), clause 8.9, paragraphes a), c), d) et e); module 3: clause 8.1, paragraphes a), c) et d) et clause 8.9, paragraphes a), c), d), e), f) et g); module 4: clause 8.1, paragraphe b), et clause 8.3, paragraphe b);

(iii) clause 9 - module 2: clause 9, paragraphes a), c), d) et e); module 3: clause 9, paragraphes a) c), d) et e);

(iv) clause 12 - module 1: clause 12, paragraphes a) et d); modules 2 et 3: clause 12, paragraphes a), d) et f);

(v) clause 13;

(vi) clause 15.1, paragraphes c), d) et e);

(vii) clause 16, paragraphe e);

(viii) clause 18 - modules 1, 2 et 3: clause 18, paragraphes a) et b); module 4: clause 18.

(b) Le paragraphe a) est sans préjudice des droits des personnes concernées au titre du règlement (UE) 2016/679.

Clause 4
Interprétation

(a) Lorsque les présentes clauses utilisent des termes définis dans le règlement (UE) 2016/679, ceux-ci ont la même signification que dans ledit règlement.

(b) Les présentes clauses sont lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679.

© Les présentes clauses ne sont pas interprétées dans un sens contraire aux droits et obligations prévus dans le règlement (UE) 2016/679.

Clause 5
Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes entre les parties existant au moment où les présentes clauses sont convenues, ou souscrites par la suite, les présentes clauses prévalent.

Clause 6
Description du ou des transferts

Les détails du ou des transferts, en particulier les catégories de données à caractère personnel qui sont transférées et la ou les finalités pour lesquelles elles le sont, sont précisés à l'annexe I.B.

Clause 7 - Facultative
Clause d'adhésion

(a) Une entité qui n'est pas partie aux présentes clauses peut, avec l'accord des parties, y adhérer à tout moment, soit en tant qu'exportateur de données soit en tant qu'importateur de données, en remplissant l'appendice et en signant l'annexe I.A.

(b) Une fois l'appendice rempli et l'annexe I.A. signée, l'entité adhérente devient partie aux présentes

clauses et a les droits et obligations d'un exportateur de données ou d'un importateur de données selon sa désignation dans l'annexe I.A.

(c) L'entité adhérente n'a aucun droit ni obligation découlant des présentes clauses pour la période antérieure à son adhésion à celles-ci.

SECTION II – OBLIGATIONS DES PARTIES

Clause 8
Garanties en matière de protection des données

L'exportateur de données garantit qu'il a entrepris des démarches raisonnables pour s'assurer que l'importateur de données est à même, par la mise en œuvre de mesures techniques et organisationnelles appropriées, de satisfaire aux obligations qui lui incombent en vertu des présentes clauses.

8.1 Instructions

(a) L'exportateur de données a informé l'importateur de données qu'il agit en qualité de sous-traitant sur instructions de son ou ses responsables du traitement, instructions qu'il met à la disposition de l'importateur de données avant le traitement.

(b) L'importateur de données ne traite les données à caractère personnel que sur instructions documentées du responsable du traitement, telles qu'elles lui ont été communiquées par l'exportateur de données, ainsi que sur instructions documentées supplémentaires de l'exportateur de données. Ces instructions supplémentaires ne sont pas en contradiction avec les instructions du responsable du traitement. Le responsable du traitement ou l'exportateur de données peut donner d'autres instructions documentées concernant le traitement des données pendant toute la durée du contrat.

(c) S'il n'est pas en mesure de suivre ces instructions, l'importateur de données en informe immédiatement l'exportateur de données. Lorsque l'importateur de données n'est pas en mesure de suivre les instructions du responsable du traitement, l'exportateur de données en informe immédiatement ce dernier.

(d) L'exportateur de données garantit qu'il a imposé à l'importateur de données les mêmes obligations en matière de protection des données que celles fixées dans le contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre entre le responsable du traitement et l'exportateur de données.

8.2 Limitation des finalités

L'importateur de données traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du transfert, telles que précisées à l'annexe I.B, sauf en cas d'instructions supplémentaires du responsable du traitement, telle qu'elles lui ont été communiquées par l'exportateur de données, ou de l'exportateur de données.

8.3 Transparence

Sur demande, l'exportateur de données met gratuitement à la disposition de la personne concernée une copie des présentes clauses, notamment de l'appendice tel que rempli par les parties. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les données à caractère personnel, l'exportateur de données peut occulter une partie du texte de l'appendice avant d'en communiquer une copie, mais fournit un résumé valable s'il serait autrement impossible, pour la personne concernée, d'en comprendre le contenu ou d'exercer ses droits. Les parties fournissent à la personne concernée, à la demande de celle-ci, les motifs des occultations, dans la mesure du possible sans révéler les

informations occultées.

8.4 Exactitude

Si l'importateur de données se rend compte que les données à caractère personnel qu'il a reçues sont inexactes, ou sont obsolètes, il en informe l'exportateur de données dans les meilleurs délais. Dans ce cas, l'importateur de données coopère avec l'exportateur de données pour rectifier ou effacer les données.

8.5 Durée du traitement et effacement ou restitution des données

Le traitement par l'importateur de données n'a lieu que pendant la durée précisée à l'annexe I.B. Au terme de la prestation des services de traitement, l'importateur de données, à la convenance de l'exportateur de données, efface toutes les données à caractère personnel traitées pour le compte du responsable du traitement et en apporte la preuve à l'exportateur de données, ou lui restitue toutes les données à caractère personnel traitées pour son compte et efface les copies existantes. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données à caractère personnel que dans la mesure où et aussi longtemps que cette législation locale l'exige. Ceci est sans préjudice de la clause 14, en particulier de l'obligation imposée à l'importateur de données par la clause 14, paragraphe e), d'informer l'exportateur de données, pendant toute la durée du contrat, s'il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences de la clause 14, paragraphe a).

8.6 Sécurité du traitement

(a) L'importateur de données et, durant la transmission, l'exportateur de données mettent en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données, notamment pour les protéger d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à ces données (ci-après la «violation de données à caractère personnel»). Lors de l'évaluation du niveau de sécurité approprié, ils tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et de la ou des finalités du traitement ainsi que des risques inhérents au traitement pour la personne concernée. Les parties envisagent en particulier de recourir au chiffrement ou à la pseudonymisation, notamment pendant la transmission, lorsque la finalité du traitement peut être atteinte de cette manière. En cas de pseudonymisation, les informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée précise restent, dans la mesure du possible, sous le contrôle exclusif de l'exportateur de données ou du responsable du traitement. Pour s'acquitter des obligations qui lui incombent en vertu du présent paragraphe, l'importateur de données met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe II. Il procède à des contrôles réguliers pour s'assurer que ces mesures continuent d'offrir le niveau de sécurité approprié.

(b) L'importateur de données ne donne l'accès aux données aux membres de son personnel que dans la mesure strictement nécessaire à la mise en œuvre, à la gestion et au suivi du contrat. Il veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

(c) En cas de violation de données à caractère personnel concernant des données à caractère personnel traitées par l'importateur de données au titre des présentes clauses, ce dernier prend des mesures appropriées pour remédier à la violation, y compris des mesures visant à en atténuer les effets négatifs. L'importateur de données informe également, dans les meilleurs délais, l'exportateur de données et, s'il y a lieu et dans la mesure du possible, le responsable du traitement après avoir eu connaissance de la violation. Cette notification contient les coordonnées d'un point de contact auprès duquel il est possible d'obtenir plus d'informations, ainsi qu'une description de la nature de la violation (y compris, si possible, les catégories et le

nombre approximatif de personnes concernées et d'enregistrements de données à caractère personnel concernés), de ses conséquences probables et des mesures prises ou proposées pour y remédier, y compris des mesures visant à en atténuer les effets négatifs potentiels. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et les autres informations sont fournies par la suite, dans les meilleurs délais, à mesure qu'elles deviennent disponibles.

(d) L'importateur de données coopère avec l'exportateur de données et l'aide afin de lui permettre de respecter les obligations qui lui incombent en vertu du règlement (UE) 2016/679, notamment celle d'informer son responsable du traitement afin que ce dernier puisse à son tour informer l'autorité de contrôle compétente et les personnes concernées, compte tenu de la nature du traitement et des informations à la disposition de l'importateur de données.

8.7 Données sensibles

Lorsque le transfert concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne, ou des données relatives à des condamnations pénales et à des infractions (ci-après les «données sensibles»), l'importateur de données applique les restrictions particulières et/ou les garanties supplémentaires indiquées à l'annexe I.B.

8.8 Transferts ultérieurs

L'importateur de données ne divulgue les données à caractère personnel à un tiers que sur instructions documentées du responsable du traitement, telles qu'elles lui ont été communiquées par l'exportateur de données. En outre, les données ne peuvent être divulguées à un tiers situé en dehors de l'Union européenne (dans le même pays que l'importateur de données ou dans un autre pays tiers, ci-après «transfert ultérieur»), que si le tiers est lié par les présentes clauses ou accepte de l'être, en vertu du module approprié, ou si:

(i) le transfert ultérieur est effectué vers un pays bénéficiant d'une décision d'adéquation en vertu de l'article 45 du règlement (UE) 2016/679 qui couvre le transfert ultérieur;

(ii) le tiers offre d'une autre manière des garanties appropriées conformément aux articles 46 ou 47 du règlement (UE) 2016/679;

(iii) le transfert ultérieur est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dans le contexte de procédures administratives, réglementaires ou judiciaires spécifiques; ou

(iv) le transfert ultérieur est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Tout transfert ultérieur est soumis au respect, par l'importateur de données, de toutes les autres garanties au titre des présentes clauses, en particulier de la limitation des finalités.

8.9 Documentation et conformité

(a) L'importateur de données traite rapidement et de manière appropriée les demandes de renseignements de l'exportateur de données ou du responsable du traitement concernant le traitement au titre des présentes clauses.

(b) Les parties sont en mesure de démontrer le respect des présentes clauses. En particulier, l'importateur de données conserve une trace documentaire appropriée des activités de traitement menées pour le compte du responsable du traitement.

(c) L'importateur de données met toutes les informations nécessaires pour démontrer le respect des obligations prévues par les présentes clauses à la disposition de l'exportateur de données, qui les transmet au responsable du traitement.

(d) L'importateur de données permet la réalisation, par l'exportateur de données, d'audits des activités de traitement couvertes par les présentes clauses, et contribue à ces audits, à intervalles raisonnables ou s'il existe des indications de non-respect. Il en est de même lorsque l'exportateur de données demande un audit sur instructions du responsable du traitement. Lorsqu'il décide d'un audit, l'exportateur de données peut tenir compte des certifications pertinentes détenues par l'importateur de données.

(e) Lorsque l'audit est effectué sur instructions du responsable du traitement, l'exportateur de données met les résultats à la disposition de ce dernier.

(f) L'exportateur de données peut choisir de procéder à l'audit lui-même ou de mandater un auditeur indépendant. Les audits peuvent comprendre des inspections dans les locaux ou les installations physiques de l'importateur de données et sont, le cas échéant, effectués avec un préavis raisonnable.

(g) Les parties mettent à la disposition de l'autorité de contrôle compétente, à la demande de celle-ci, les informations mentionnées aux paragraphes b) et c), y compris les résultats de tout audit.

Clause 9

Recours à des sous-traitants ultérieurs

(a) L'importateur de données a l'autorisation générale du responsable du traitement de recruter un ou plusieurs sous-traitants ultérieurs à partir d'une liste arrêtée d'un commun accord. L'importateur de données informe expressément par écrit le responsable du traitement de tout changement concernant l'ajout ou le remplacement de sous-traitants ultérieurs qu'il est prévu d'apporter à cette liste au moins [précisez le délai] à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour émettre des objections à l'encontre de ces changements avant le recrutement du ou des sous-traitants ultérieurs. L'importateur de données fournit au responsable du traitement les informations nécessaires pour permettre à ce dernier d'exercer son droit d'émettre des objections. L'importateur de données informe l'exportateur de données du recrutement du ou des sous-traitants ultérieurs.

(b) Lorsque l'importateur de données recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat écrit qui prévoit, en substance, les mêmes obligations en matière de protection des données que celles qui lient l'importateur de données en vertu des présentes clauses, notamment en ce qui concerne les droits du tiers bénéficiaire pour les personnes concernées . Les parties conviennent qu'en respectant la présente clause, l'importateur de données satisfait aux obligations qui lui incombent en vertu de la clause 8.8. L'importateur de données veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses.

(c) L'importateur de données fournit sur demande, à l'exportateur de données ou au responsable du traitement, une copie du contrat avec le sous-traitant ultérieur et de ses éventuelles modifications ultérieures. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les données à caractère personnel, l'importateur de données peut occulter une partie du texte du contrat avant d'en communiquer une copie.

(d) L'importateur de données reste pleinement responsable à l'égard de l'exportateur de données de l'exécution des obligations qui incombent au sous-traitant ultérieur en vertu du contrat qu'il a conclu avec lui. L'importateur de données notifie à l'exportateur de données tout manquement du sous-traitant ultérieur aux obligations qui lui incombent en vertu dudit contrat.

(e) L'importateur de données convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire en

vertu de laquelle, dans les cas où l'importateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'exportateur de données a le droit de résilier le contrat du sous-traitant ultérieur et de donner instruction à ce dernier d'effacer ou de restituer les données à caractère personnel.

Clause 10

Droits des personnes concernées

(a) L'importateur de données informe sans délai l'exportateur de données et, s'il y a lieu, le responsable du traitement de toute demande reçue d'une personne concernée, mais n'y répond pas à moins d'y avoir été autorisé par le responsable du traitement.

(b) L'importateur de données aide, si nécessaire en coopération avec l'exportateur de données, le responsable du traitement à s'acquitter de son obligation de répondre aux demandes de personnes concernées désireuses d'exercer leurs droits en vertu du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725, selon le cas. À cet égard, les parties indiquent à l'annexe II les mesures techniques et organisationnelles appropriées, compte tenu de la nature du traitement, au moyen desquelles l'aide sera fournie, ainsi que la portée et l'étendue de l'aide requise.

(c) Lorsqu'il s'acquitte des obligations qui lui incombent en vertu des paragraphes a) et b), l'importateur de données se conforme aux instructions du responsable du traitement, telles qu'elles lui ont été communiquées par l'exportateur de données.

Clause 11

Voies de recours

(a) L'importateur de données informe les personnes concernées, sous une forme transparente et aisément accessible, au moyen d'une notification individuelle ou sur son site web, d'un point de contact autorisé à traiter les réclamations. Il traite sans délai toute réclamation reçue d'une personne concernée.

(b) En cas de litige entre une personne concernée et l'une des parties portant sur le respect des présentes clauses, cette partie met tout en œuvre pour parvenir à un règlement à l'amiable dans les meilleurs délais. Les parties se tiennent mutuellement informées de ces litiges et, s'il y a lieu, coopèrent pour les résoudre.

(c) Lorsque la personne concernée invoque un droit du tiers bénéficiaire en vertu de la clause 3, l'importateur de données accepte la décision de la personne concernée:

(i) d'introduire une réclamation auprès de l'autorité de contrôle de l'État membre dans lequel se trouve sa résidence habituelle ou son lieu de travail, ou auprès de l'autorité de contrôle compétente au sens de la clause 13;

(ii) de renvoyer le litige devant les juridictions compétentes au sens de la clause 18.

(d) Les parties acceptent que la personne concernée puisse être représentée par un organisme, une organisation ou une association à but non lucratif dans les conditions énoncées à l'article 80, paragraphe 1, du règlement (UE) 2016/679.

(e) L'importateur de données se conforme à une décision qui est contraignante en vertu du droit applicable de l'Union ou d'un État membre.

(f) L'importateur de données convient que le choix effectué par la personne concernée ne remettra pas en cause le droit procédural et matériel de cette dernière d'obtenir réparation conformément à la législation applicable.

Clause 12

Responsabilité

(a) Chaque partie est responsable envers la ou les autres parties des dommages qu'elle cause à l'autre ou aux autres parties du fait d'un manquement aux présentes clauses.

(b) L'importateur de données est responsable à l'égard de la personne concernée, et la personne concernée a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par l'importateur de données ou son sous-traitant ultérieur du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses.

(c) Nonobstant le paragraphe b), l'exportateur de données est responsable à l'égard de la personne concernée et celle-ci a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par l'exportateur de données ou l'importateur de données (ou son sous-traitant ultérieur) du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses. Ceci est sans préjudice de la responsabilité de l'exportateur de données et, si l'exportateur de données est un sous-traitant agissant pour le compte d'un responsable du traitement, de la responsabilité de ce dernier au titre du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725, selon le cas.

(d) Les parties conviennent que, si l'exportateur de données est reconnu responsable, en vertu du paragraphe c), du dommage causé par l'importateur de données (ou son sous-traitant ultérieur), il a le droit de réclamer auprès de l'importateur de données la part de la réparation correspondant à la responsabilité de celui-ci dans le dommage.

(e) Lorsque plusieurs parties sont responsables d'un dommage causé à la personne concernée du fait d'une violation des présentes clauses, toutes les parties responsables le sont conjointement et solidairement et la personne concernée a le droit d'intenter une action en justice contre n'importe laquelle de ces parties.

(f) Les parties conviennent que, si la responsabilité d'une d'entre elles est reconnue en vertu du paragraphe e), celle-ci a le droit de réclamer auprès de l'autre ou des autres parties la part de la réparation correspondant à sa/leur responsabilité dans le dommage.

(g) L'importateur de données ne peut invoquer le comportement d'un sous-traitant ultérieur pour échapper à sa propre responsabilité.

Clause 13
Contrôle

(a) [Si l'exportateur de données est établi dans un État membre de l'Union:] L'autorité de contrôle chargée de garantir le respect, par l'exportateur de données, du règlement (UE) 2016/679 en ce qui concerne le transfert de données, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité de contrôle compétente.

[Si l'exportateur de données n'est pas établi dans un État membre de l'Union, mais relève du champ d'application territorial du règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2, et a désigné un représentant en vertu de l'article 27, paragraphe 1, dudit règlement:] L'autorité de contrôle de l'État membre dans lequel le représentant au sens de l'article 27, paragraphe 1, du règlement (UE) 2016/679 est établi, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité de contrôle compétente.

[Si l'exportateur de données n'est pas établi dans un État membre de l'Union, mais relève du champ d'application territorial du règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2 sans toutefois avoir à désigner un représentant en vertu de l'article 27, paragraphe 2, du règlement (UE) 2016/679:] L'autorité de contrôle d'un des États membres dans lesquels se trouvent les personnes concernées dont les

données à caractère personnel sont transférées au titre des présentes clauses en lien avec l'offre de biens ou de services ou dont le comportement fait l'objet d'un suivi, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité compétente.

(b) L'importateur de données accepte de se soumettre à la juridiction de l'autorité de contrôle compétente et de coopérer avec elle dans le cadre de toute procédure visant à garantir le respect des présentes clauses. En particulier, l'importateur de données accepte de répondre aux demandes de renseignements, de se soumettre à des audits et de se conformer aux mesures adoptées par l'autorité de contrôle, notamment aux mesures correctrices et compensatoires. Il confirme par écrit à l'autorité de contrôle que les mesures nécessaires ont été prises.

SECTION III – LÉGISLATIONS LOCALES ET OBLIGATIONS EN CAS D'ACCÈS DES AUTORITÉS PUBLIQUES

Clause 14
Législations et pratiques locales ayant une incidence sur le respect des clauses

(a) Les parties garantissent qu'elles n'ont aucune raison de croire que la législation et les pratiques du pays tiers de destination applicables au traitement des données à caractère personnel par l'importateur de données, notamment les exigences en matière de divulgation de données à caractère personnel ou les mesures autorisant l'accès des autorités publiques à ces données, empêchent l'importateur de données de s'acquitter des obligations qui lui incombent en vertu des présentes clauses. Cette disposition repose sur l'idée que les législations et les pratiques qui respectent l'essence des libertés et droits fondamentaux et qui n'excèdent pas ce qui est nécessaire et proportionné dans une société démocratique pour préserver un des objectifs énumérés à l'article 23, paragraphe 1, du règlement (UE) 2016/679 ne sont pas en contradiction avec les présentes clauses.

(b) Les parties déclarent qu'en fournissant la garantie mentionnée au paragraphe a), elles ont dûment tenu compte, en particulier, des éléments suivants:

(i) des circonstances particulières du transfert, parmi lesquelles la longueur de la chaîne de traitement, le nombre d'acteurs concernés et les canaux de transmission utilisés; les transferts ultérieurs prévus; le type de destinataire; la finalité du traitement; les catégories et le format des données à caractère personnel transférées; le secteur économique dans lequel le transfert a lieu et le lieu de stockage des données transférées;

(ii) des législations et des pratiques du pays tiers de destination – notamment celles qui exigent la divulgation de données aux autorités publiques ou qui autorisent l'accès de ces dernières aux données – pertinentes au regard des circonstances particulières du transfert, ainsi que des limitations et des garanties applicables[2] ;

(iii) de toute garantie contractuelle, technique ou organisationnelle pertinente mise en place pour

2 En ce qui concerne l'incidence de ces législations et pratiques sur le respect des présentes clauses, différents éléments peuvent être considérés comme faisant partie d'une évaluation globale. Ces éléments peuvent inclure une expérience concrète, documentée et pertinente de cas antérieurs de demandes de divulgation émanant d'autorités publiques, ou l'absence de telles demandes, couvrant un laps de temps suffisamment représentatif. Il peut s'agir de registres internes ou d'autres documents établis de manière continue conformément au principe de diligence raisonnable et certifiés à un niveau hiérarchique élevé, pour autant que ces informations puissent être partagées légalement avec des tiers. Lorsque cette expérience pratique est invoquée pour conclure que l'importateur de données ne sera pas empêché de respecter les présentes clauses, il y a lieu de l'étayer par d'autres éléments pertinents et objectifs, et il appartient aux parties d'examiner avec soin si ces éléments, pris dans leur ensemble, ont un poids suffisant, du point de vue de leur fiabilité et de leur représentativité, pour soutenir cette conclusion. En particulier, les parties doivent s'assurer que leur expérience pratique est corroborée et non contredite par des informations fiables accessibles au public ou disponibles d'une autre manière sur l'existence ou l'absence de demandes dans le même secteur et/ou sur l'application pratique du droit, comme la jurisprudence et les rapports d'organes de contrôle indépendants.

compléter les garanties prévues par les présentes clauses, y compris les mesures appliquées pendant la transmission et au traitement des données à caractère personnel dans le pays de destination.

(c) L'importateur de données garantit que, lors de l'évaluation au titre du paragraphe b), il a déployé tous les efforts possibles pour fournir des informations pertinentes à l'exportateur de données et convient qu'il continuera à coopérer avec ce dernier pour garantir le respect des présentes clauses.

(d) Les parties conviennent de conserver une trace documentaire de l'évaluation au titre du paragraphe b) et de mettre cette évaluation à la disposition de l'autorité de contrôle compétente si celle-ci en fait la demande.

(e) L'importateur de données accepte d'informer sans délai l'exportateur de données si, après avoir souscrit aux présentes clauses et pendant la durée du contrat, il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences du paragraphe a), notamment à la suite d'une modification de la législation du pays tiers ou d'une mesure (telle qu'une demande de divulgation) indiquant une application pratique de cette législation qui n'est pas conforme aux exigences du paragraphe a). l'exportateur de données transmet la notification au responsable du traitement.

(f) À la suite d'une notification au titre du paragraphe e), ou si l'exportateur de données a d'autres raisons de croire que l'importateur de données ne peut plus s'acquitter des obligations qui lui incombent en vertu des présentes clauses, l'exportateur de données définit sans délai les mesures appropriées (par exemple des mesures techniques ou organisationnelles visant à garantir la sécurité et la confidentialité) qu'il doit adopter et/ou qui doivent être adoptées par l'importateur de données pour remédier à la situation, si nécessaire en concertation avec le responsable du traitement. L'exportateur de données suspend le transfert de données s'il estime qu'aucune garantie appropriée ne peut être fournie pour ce transfert ou si le responsable du traitement ou l'autorité de contrôle compétente lui en donne donnent l'instruction. Dans ce cas, l'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement. Lorsque le contrat est résilié en vertu de la présente clause, la clause 16, paragraphes d) et e), s'applique.

Clause 15

Obligations de l'importateur de données en cas d'accès des autorités publiques

15.1 Notification

(a) L'importateur de données convient d'informer sans délai l'exportateur de données et, si possible, la personne concernée (si nécessaire avec l'aide de l'exportateur de données):

(i) s'il reçoit une demande juridiquement contraignante d'une autorité publique, y compris judiciaire, en vertu de la législation du pays de destination en vue de la divulgation de données à caractère personnel transférées au titre des présentes clauses; cette notification comprend des informations sur les données à caractère personnel demandées, l'autorité requérante, la base juridique de la demande et la réponse fournie; ou

(ii) s'il a connaissance d'un quelconque accès direct des autorités publiques aux données à caractère personnel transférées au titre des présentes clauses en vertu de la législation du pays de destination; cette notification comprend toutes les informations dont l'importateur de données dispose.
L'exportateur de données transmet la notification au responsable du traitement.

(b) Si la législation du pays de destination interdit à l'importateur de données d'informer l'exportateur de données et/ou la personne concernée, l'importateur de données convient de tout mettre en œuvre pour obtenir une levée de cette interdiction, en vue de communiquer autant d'informations que possible, dans les

meilleurs délais. L'importateur de données accepte de garder une trace documentaire des efforts qu'il a déployés afin de pouvoir en apporter la preuve à l'exportateur de données, si celui-ci lui en fait la demande.

(c) Lorsque la législation du pays de destination le permet, l'importateur de données accepte de fournir à l'exportateur de données, à intervalles réguliers pendant la durée du contrat, autant d'informations utiles que possible sur les demandes reçues (notamment le nombre de demandes, le type de données demandées, la ou les autorités requérantes, la contestation ou non des demandes et l'issue de ces contestations, etc.). L'exportateur de données transmet les informations au responsable du traitement.

(d) L'importateur de données accepte de conserver les informations mentionnées aux paragraphes a) à c) pendant la durée du contrat et de les mettre à la disposition de l'autorité de contrôle compétente si celle-ci lui en fait la demande.

(e) Les paragraphes a) à c) sont sans préjudice de l'obligation incombant à l'importateur de données, en vertu de la clause 14, paragraphe e), et de la clause 16, d'informer sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses.

15.2 Contrôle de la légalité et minimisation des données

(a) L'importateur de données accepte de contrôler la légalité de la demande de divulgation, en particulier de vérifier si elle s'inscrit dans les limites des pouvoirs conférés à l'autorité publique requérante, et de la contester si, après une évaluation minutieuse, il conclut qu'il existe des motifs raisonnables de considérer qu'elle est illégale en vertu de la législation du pays de destination, des obligations applicables en vertu du droit international et des principes de courtoisie internationale. L'importateur de données exerce les possibilités d'appel ultérieures dans les mêmes conditions. Lorsqu'il conteste une demande, l'importateur de données demande des mesures provisoires visant à suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente se prononce sur son bien-fondé. Il ne divulgue pas les données à caractère personnel demandées tant qu'il n'est pas obligé de le faire en vertu des règles de procédure applicables. Ces exigences sont sans préjudice des obligations incombant à l'importateur de données en vertu de la clause 14, paragraphe e).

(b) L'importateur de données accepte de garder une trace documentaire de son évaluation juridique ainsi que de toute contestation de la demande de divulgation et, dans la mesure où la législation du pays de destination le permet, de mettre les documents concernés à la disposition de l'exportateur de données. Il les met également à la disposition de l'autorité de contrôle compétente si celle-ci lui en fait la demande. L'exportateur de données met l'évaluation à la disposition du responsable du traitement.

(c) L'importateur de données accepte de fournir le minimum d'informations autorisé lorsqu'il répond à une demande de divulgation, sur la base d'une interprétation raisonnable de la demande.

SECTION IV — DISPOSITIONS FINALES

Clause 16
Non-respect des clauses et résiliation

(a) L'importateur de données informe sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses, quelle qu'en soit la raison.

(b) Dans le cas où l'importateur de données enfreint les présentes clauses ou n'est pas en mesure de les respecter, l'exportateur de données suspend le transfert de données à caractère personnel à l'importateur de données jusqu'à ce que le respect des présentes clauses soit à nouveau garanti ou que le contrat soit résilié. Ceci est sans préjudice de la clause 14, paragraphe f).

(c) L'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses, lorsque:

(i) l'exportateur de données a suspendu le transfert de données à caractère personnel à l'importateur de données en vertu du paragraphe b) et que le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension;

(ii) l'importateur de données enfreint gravement ou de manière persistante les présentes clauses; ou

(iii) l'importateur de données ne se conforme pas à une décision contraignante d'une juridiction ou d'une autorité de contrôle compétente concernant les obligations qui lui incombent au titre des présentes clauses.

Dans ces cas, il informe l'autorité de contrôle compétente et le responsable du traitement de ce non-respect. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement.

(d) Les données à caractère personnel qui ont été transférées avant la résiliation du contrat au titre du paragraphe c) sont immédiatement restituées à l'exportateur de données ou effacées dans leur intégralité, à la convenance de celui-ci. Il en va de même pour toute copie des données. L'importateur de données apporte la preuve de l'effacement des données à l'exportateur de données. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel transférées, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données que dans la mesure où et aussi longtemps que cette législation locale l'exige.

(e) Chaque partie peut révoquer son consentement à être liée par les présentes clauses i) si la Commission européenne adopte une décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 qui couvre le transfert de données à caractère personnel auquel les présentes clauses s'appliquent; ou ii) si le règlement (UE) 2016/679 est intégré dans le cadre juridique du pays vers lequel les données à caractère personnel sont transférées. Ceci est sans préjudice des autres obligations qui s'appliquent au traitement en question en vertu du règlement (UE) 2016/679.

Clause 17

Droit applicable

Les présentes clauses sont régies par le droit d'un des États membres de l'Union européenne, pour autant que ce droit reconnaisse des droits au tiers bénéficiaire. Les parties conviennent qu'il s'agit du droit de la France.

Clause 18

Élection de for et juridiction

(a) Tout litige survenant du fait des présentes clauses est tranché par les juridictions d'un État membre de l'Union européenne.

(b) Les parties conviennent qu'il s'agit des juridictions de la France.

(c) La personne concernée peut également poursuivre l'exportateur et/ou l'importateur de données devant les juridictions de l'État membre dans lequel elle a sa résidence habituelle.

(d) Les parties acceptent de se soumettre à la compétence de ces juridictions.

APPENDICE

ANNEXE I

A. LISTE DES PARTIES

Exportateur(s) de données: [Identité et coordonnées du ou des exportateurs de données et, le cas échéant, de leur délégué à la protection des données et/ou de leur représentant dans l'Union européenne]
1. Nom: ...
Adresse: ...
Nom, fonction et coordonnées de la personne de contact: ...
Activités en rapport avec les données transférées au titre des présentes clauses: ...
Signature et date: ...
Rôle (responsable du traitement/sous-traitant): ...

2. ...

Importateur(s) de données: [Identité et coordonnées du ou des importateurs de données, y compris de toute personne de contact chargée de la protection des données]
1. Nom: ...
Adresse: ...
Nom, fonction et coordonnées de la personne de contact: ...
Activités en rapport avec les données transférées au titre des présentes clauses: ...
Signature et date: ...
Rôle (responsable du traitement/sous-traitant): ...

2. ...

B. DESCRIPTION DU TRANSFERT

Catégories de personnes concernées dont les données à caractère personnel sont transférées
.....
Catégories de données à caractère personnel transférées
.....
Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, telles que la limitation stricte des finalités, les restrictions d'accès (notamment l'accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.
.....
Fréquence du transfert (indiquez, par exemple, si les données sont transférées sur une base ponctuelle ou continue).
.....
Nature du traitement
.....
Finalité(s) du transfert et du traitement ultérieur des données
.....
Durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, critères utilisés pour déterminer cette durée
.....
Pour les transferts à des sous-traitants (ultérieurs), veuillez également préciser l'objet, la nature et la durée du traitement
.....

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

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

ANNEXE II
MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS LES MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À GARANTIR LA SÉCURITÉ DES DONNÉES

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's Information Security program is designed to direct and maintain the organization's information security strategy and controls. This system ensures enterprise-wide compliance with HP's security policies and controls, as well as adherence to the security requirements of its customers. Structured in alignment with industry-standard cybersecurity frameworks, laws, and regulations, the Framework is reviewed annually to adapt to HP's evolving thread landscape.

3. Cybersecurity Risk Management

HP's cybersecurity risk management program is designed to preserve the confidentiality, integrity, and availability of its information assets. The program provides a consistent approach to identifying, assessing, prioritizing, treating, remedying, tracking, and reporting cybersecurity risks. HP defines its Risk Appetite as the acceptable level of loss exposure and Risk Tolerance as the degree of variance from this appetite. Risks are evaluated using a defined methodology, enabling HP to mitigate information security risks to an acceptable level. This program aligns with HP's Enterprise Risk Management process.

4. HR Security

HP Human Resource Security policy ensures information security throughout the employee lifecycle by establishing processes for access to facilities, information systems, and other assets. This includes obtaining written acknowledgments through confidentiality and non-disclosure agreements, as well as conducting background screening procedures. All candidates for employment with HP must complete a background verification check in accordance with relevant laws, regulations, and ethics.

5. Asset Management

HP has a process for identifying technical information assets, categorizing critical assets, and maintaining documented handling procedures for each information classification type, including those containing Personal Data. These procedures cover storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification. HP security policies and standards also mandate the secure disposal of media.

6. Data Security

HP's Data Security program outlines the security practices and technical controls that must be implemented to protect the confidentiality, authenticity, and integrity of data. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification are a few of the factors that determine how information is classified under HP's Data Security policy. In addition to data handling procedures, the policy outlines data encryption, deletion, collection and processing, retention, backup, and data loss prevention.

7. Access Control

HP employs the principle of least privilege for logical access control, providing user access through unique user IDs and passwords. The password policy defines complexity, strength, validity, and password-history controls. Access rights are periodically reviewed and revoked upon personnel departure. Agreed-upon procedures for user account creation and deletion are implemented to grant and revoke access to client

systems during engagements.

8. 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. Our Cryptography program involves the use of mathematical techniques to secure information and communications, ensuring that only authorized parties can access the data. A critical component of HP's information security program is protecting data from unauthorized access and tampering.

9. Physical and Environmental Security

HP facilities are secured using various physical and electronic access controls, including security guards, electronic access control, and closed-circuit television (CCTV). Facilities are also equipped with necessary infrastructure support, including temperature control and power backups, using UPS and/or diesel generators to support critical services. All HP personnel are registered and required to carry appropriate identification badges.

10. Operations Management

HP has established minimum hardening requirements for technology infrastructure, including workstations, servers, and network equipment. These devices use pre-hardened operating system images, with requirements varying by operating system and implemented controls. Additionally, HP has deployed Network Intrusion Detection/Prevention Systems (NIDS/NIPS) that are monitored and managed 24/7.

11. Communications Security

Communications Security ensures the protection of information within corporate networks. This includes the installation and management of network security components (e.g., firewalls), segregation of networks, as well as web filtering and email handling controls. Additionally, it involves monitoring and managing communication channels to detect and prevent unauthorized access or data breaches.

12. Systems Security

HP's policy mandates a secure development methodology for systems and software throughout their lifecycle. The Software Development Lifecycle covers initiation, development/acquisition, implementation, operations, and disposal. All system components are evaluated for their impact on overall security. HP has established controls for application service transactions, including user credential validation, digital signatures, encryption, secure communication protocols, and storing transaction details within the appropriate network security zone. Regular internal vulnerability scans are also performed.

13. Third Parties and Subcontractors

HP has processes in place to select sub-contractors who comply with comprehensive contractual security requirements. For applicable suppliers handling HP or customer data, or accessing the HP network, HP Cybersecurity conducts a risk assessment to verify an information security program with physical, technical, and administrative safeguards. This assessment is required before the supplier can access HP information.

14. Information Security Incident Management

HP has a comprehensive Cyber Incident Management Process that outlines purpose, scope, roles, responsibilities, management commitment, organizational coordination, implementation procedures, and compliance checking. This process is reviewed and updated annually. The Cyber Incident Response Team, including HP Cybersecurity personnel trained in incident response and crisis management, conducts regular tabletop reviews of the process and any incidents or events.

15. Business Continuity Management

HP's global Continuity of Operations program ensures end-to-end continuity through collaborative, standardized, and documented planning processes. The company periodically exercises its business continuity plans to ensure effectiveness, testing and updating all plans at least yearly. Additionally, all personnel involved in the business continuity plan receive proper training.

16. Compliance

Compliance shapes HP's approach to meeting legal, contractual, and internal expectations for an effective information security program. Regular information security reviews ensure protocols are integrated into each business group's operations. The review process also keeps documents updated to reflect current legal obligations as requirements evolve.

17. Payment Card Industry

The Payment Card Industry (PCI) framework guides HP's approach to achieving PCI Compliance, outlining business responsibilities and security controls aligned with PCI DSS. By installing and maintaining network security controls like firewalls, HP ensures it meets PCI Compliance requirements.

18. HP Product Security

HP Product Security encompasses essential practices to secure HP Products, such as code signing, managing product security vulnerabilities, issuing security bulletins, and reporting product security issues. These measures ensure that HP products remain secure and reliable for users. Product security is of paramount importance at HP, as it helps maintain customer trust and protects against potential threats.

19. HP Service Security

HP Service Security encompasses essential practices to secure the services provided to HP customers. This policy addresses various areas of service security, including HP infrastructure hosted, third-party hosted, partner hosted, and customer hosted environments. These measures ensure that HP services remain secure and reliable for users. By implementing robust security practices, HP ensures the safety and integrity of its products and services, fostering a secure and trustworthy environment for all users.

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.

Appendice 4

Accord International sur le Transfert de Données (IDTA) (RU)

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 Contact details including email: 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
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 T ransferred 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.

Appendice 5

Clauses Contractuelles Types (Argentine)

In accordance with the provisions of clause 6.4.1 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 4 shall be amended by adding the following:*

Where these Clauses use terms that are defined in Argentina's Data Protection Law No. 25.326, its regulatory Decree No. 1558/2001, and their complementary regulations (as amended or replaced from time to time), such as 'personal data', 'sensitive data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority', those terms shall have the same meaning as set forth in those regulations (as amended or replaced from time to time);

2. *For the purposes of these Clauses, references to "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;*

3. *For the purposes of these Clauses, 'the applicable data protection law' or 'Regulation (EU) 2016/679' shall be understood as references to Argentina's Data Protection Law No. 25.326 and its supporting regulations (as amended or replaced from time to time).*

4. *In addition to Clause 8.8 (Onward transfers), the following shall apply:*

Where Personal Data originating from Argentina is concerned, international data transfers shall only be permitted if either (i) the destination country provides adequate level of protection as determined by

Argentina law, or (ii) one of the exceptions under Article 12 of Argentina's Data Protection Law 25.326 applies.

5. *Clause 11, subsection (c), item (ii) shall be replaced as follows:*

(c) (ii) to refer the dispute to the judicial and administrative jurisdiction of the Argentina Republic.

6. *Clause 17 shall be replaced as follows:*

These clauses shall be governed by the laws of the Argentina Republic, in particular by the Law No. 25.326, its regulations and dispositions issued by Argentina's Data Protection Authority (as amended or replaced from time to time).

7. *Clause 18 shall be replaced as follows:*

   (a) Any dispute arising from these Clauses shall be resolved by the courts of the Argentina Republic.

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

Appendice 6

Contrat Type pour le Transfert Transfrontalier d'Informations Personnelles (Chine)

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: HP Trading (Shanghai) Co. Ltd.

Address: Room 203-A, No. 26 Jia Feng Road, Pilot Free Trade Zone, Shanghai, China

Contact Information: katherine.liu@hp.com

Contact Person: Katherine Liu Position: China Data Protection Manager

and

Overseas recipient: HP Inc.

Address: 1501 Page Mill Road, Palo Alto, California 94304 USA

Contact Information: nestor.rivera@hp.com

Contact Person: Nestor Rivera Position: SVP and Deputy General Counsel, Trust and Privacy

The personal information handler and the overseas recipient shall conduct cross-border transfer of personal information in accordance with this Contract. In terms of any commercial activities relating thereto, both Parties [have entered into]/ [agreed to enter into] a commercial contract, i.e., [the name of the commercial contract, if any] on [Year], [Month], [Date].

The text of this Contract is drawn up in accordance with the provisions of the *Measures for Standard Contract for Personal Information Cross-Border Transfer*. If there is any other agreement between the two parties, it will be described in detail, if needed, in an Annex, which would constitute an integral part of this Contract on the condition that they do not conflict with the content of this Contract.

Article 1 Definition

In this Contract, except as otherwise provided in the context:

(1) "Personal information handler" means any organization or individual who independently determines the purpose and means of Personal Information processing activities and provides personal information outside the People's Republic of China.

(2) “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.

(3) The personal information handler and the overseas recipient are hereinafter referred to individually as a “Party” and collectively as the “Parties”.

(4) “Personal information subject” refers to a natural person identified by or associated with the personal information.

(5) “Personal information” means all kinds of information related to an identified or identifiable individual, recorded in electronic form or other forms, excluding anonymized information.

(6) “Sensitive personal information” means any personal information that is likely to result in damage to the personal dignity of any individual or damage to his or her personal or property safety once leaked or illegally used, including information such as biometric identification, religious belief, specific identity, medical health, financial account and personal whereabouts, as well as the personal information of minors under the age of 14.

(7) “Regulatory authority” refers to the cyberspace departments at or above the provincial level of the People's Republic of China.

(8) “Relevant laws and regulations” refer to 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*, the *Civil Code of the People's Republic of China*, the *Civil Procedure Law of the People's Republic of China*, the *Measures for Standard Contract for Personal Information Cross-border*and other laws and regulations of the People's Republic of China.

(9) 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 shall be subject to the following obligations:

(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) The personal information subject shall be notified of the name and contact information of the overseas recipient, the processing purpose, the processing means, the category of personal information and the retention period, and the means and procedure for exercising the rights of the personal information subject etc., if necessary in an Annex titled “Instructions on Personal Information Cross-Border Transfer”. Where sensitive personal information is to be provided overseas, the personal information subject shall also be informed of the necessity of provision of sensitive personal information and its impact on the rights and interests of the personal information subject, unless otherwise provided by the laws and administrative regulations that such notification is not required.

(3) Where the provision of personal information overseas is based on individual's consent, the separate consent shall be obtained from the personal information subject. If personal information of minors under the age of 14 is involved, the separate consent shall be obtained from his or her parents or other guardians. Where the written consent is required to be obtained by laws and administrative regulations, such written consent shall be obtained.

(4) 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.

(5) It shall make reasonable efforts to ensure that the overseas recipient adopts the following technical and management measures (based on a comprehensive consideration of personal information security risks resulted from the processing purpose of the personal information, the category of personal information, scale, scope and sensitivity of personal information to be exported, the quantity and frequency of transfer, the duration of transfer and retention period of personal information by the overseas recipient etc.), to perform the obligations under this Contract:

Technical and management measures specified in an Annex, as needed.

(6) It will provide a copy of relevant legal provisions and technical standards to the overseas recipient at its/his request.

(7) It will respond to inquiries from regulatory authorities about the personal information processing activity of the overseas recipient.

(8) 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.

(9) 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.

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

(11) It will provide the regulatory authorities with the information specified in Paragraph (11) of Article 3, including all audit results, in accordance with relevant laws and regulations.

Article 3 Obligations of overseas recipient

The overseas recipient shall be subject to following obligations:

(1) It shall process personal information in accordance with the agreements listed, if needed, in an Annex titled "Instructions on Personal Information Cross-Border Transfer". Where the processing of personal information goes beyond the agreed processing purpose, processing means, and categories of personal information, the separate consent of personal information subject shall be obtained in advance if such processing is relied on the individual's consent. If any personal information of minors under the age of 14 is involved, the separate consent of minors' parents or other guardians shall be obtained.

(2) Where the overseas recipient is entrusted by the personal information handler to process personal information, it shall process personal information in accordance with the agreement with the personal information handler. The overseas recipient shall not process personal information in a way beyond the processing purpose or means as agreed with the personal information handler.

(3) 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. (4) It shall process personal information in a manner that has the least impact on the rights and interests of the personal information subject.

(5) 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. Where it is entrusted by the personal information handler to process personal information, the overseas recipient shall return the personal information to the personal information handler or delete it, in the event the entrustment contract does not come into effect, becomes invalid, or is revoked or terminated, and provide a written statement to the personal information handler. If it is technically impossible to delete the personal information, the overseas recipient shall cease the processing of personal information other than storage and any necessary measures taken for the security protection.

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

1. Take effective technical and management measures including but not limited to those set out in Article 2 (5) this Contract, and conduct periodic checks to ensure the security of personal information.

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.

(7) If the processed personal information is or may be tampered with, destroyed, leaked, lost, illegally used, provided or accessed without authorization, the overseas recipient shall carry out the following works:

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) the category of personal information that has been or may be tampered with, destroyed, leaked, lost, illegally used, provided or accessed without authorization, the cause of the adverse event, the potential damage;

(b) Remedial measures that have been taken;

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

(d) 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. Where the processing of personal information is entrusted by the personal information handler, the personal information handler shall notify the personal information subject.

4. Record and retain all information in relation to the occurrence or potential occurrence of tampering, destruction, leakage, loss, illegal use, unauthorized provision or access, including all remedial measures taken.

(8) 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, the retention period, as well as the methods and procedures for exercising the rights of the personal

information subjects. Where sensitive personal information is to be provided to such third party, the personal information subject shall also be informed of the necessity of providing sensitive personal information and its impact on personal rights and interests unless otherwise provided by the laws and administrative regulations that such notification is not required.

3. Where the processing of personal information is based on individual's consent, the separate consent of the personal information subject shall be obtained. If personal information of a minor under the age of 14 is involved, the consent shall be obtained from his or her parents or other guardians. Where written consent is required by laws or administrative regulations, such written consent shall be obtained.

4. 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 to assume liabilities for the infringement to the rights of the personal information subject arising from the provision of the personal information to the third party located outside the People's Republic of China.

5. Provide a copy of the above written agreement to the personal information subject at the request of the personal information subject. If trade secrets or confidential information are involved, the relevant contents of the written agreement can be redacted to some extent without affecting the understanding of the personal information subject.

(9) 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, if necessary, in an Annex titled "Instructions on Personal Information Cross-Border Transfer" to this Contract and supervise the personal information processing activity of that third party.

(10) Make automated decisions by using personal information, ensure the transparency of decision making and the fairness and impartiality of the results, and do not accord unreasonable differential treatment to personal information subjects on transaction conditions such as transaction prices. Where automated decision-making is used for information push and commercial marketing to the personal information subject, the overseas recipient shall provide personal information subject with either options that are not specific to their personal characteristics, or with a convenient way of refusal for the personal information subject.

(11) 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 necessary data files and documents, or to allow the personal information handler to conduct compliance audits on 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 compliance audit.

(12) 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.

(13) 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 shall ensure that they have fulfilled their obligations of reasonable care at the time of the conclusion of this Contract and have not found any personal information protection policy & regulations of the country or region where the overseas recipient is located (including any requirements for the provision of personal information or the provisions authorizing public organs to access personal information) in that would affect the overseas recipient's 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 of personal information, 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 by such country or region;

(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.

(6) The overseas recipient shall immediately notify the personal information handler when receiving the request from the government department or judicial authority of the country or region where it is located for provision of personal information under this Contract.

Article 5 Rights of personal information subjects

The Parties agree 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 of the relevant information truthfully, accurately and completely in a clear and plain language.

(4) 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.

(5) 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 (5), (6), (7) and (11) of Article 2;

2. Article 3, except Subparagraphs 2 and 4 of Paragraph (7), Paragraphs (9), (11), (12) and (13) of Article 3;

3. Article 4, except Paragraphs (5) and (6) of Article 4.

4. Article 5;

5. Article 6;

6. Paragraphs (2) and (3) of Article 8;

7. Paragraph (5) of Article 9.

The agreement above shall not affect the rights and interests of the personal information subject as provided in the *Personal Information Protection Law of the People's Republic of China*.

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:

Contact person: HP Inc. Legal, Trust and Privacy Organization

contact information: 1501 Page Mill Road, Palo Alto, California 94304, USA

(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 Article 5, the overseas recipient accepts the personal information subject to defend his or her rights through either of the following means:

1. Lodge a complaint with the regulatory authorities;

2. Bring an action in the court as provided for in Article 6 (5).

(4) The Parties agree that where personal information subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, if the personal information subject chooses to apply the Relevant Laws and Regulations of the People's Republic of China, such choice shall prevail.

(5) The Parties agree that where personal information subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, the personal information subject may bring a lawsuit with a competent court in accordance with the *Civil Procedure Law of the People's Republic of China*.

(6) The Parties agree that the fact that the personal information subject has sought remedies in accordance with provisions above shall not prejudice his/her rights to seek remedies under other laws and regulations.

Article 7 Cancellation of contract

(1) If the overseas recipient violates any of its obligations stipulated in this Contract, or is unable to perform this Contract due to any change in the personal information protection policies and regulations of the country or region where the overseas recipient is located (including amendment to the laws or the adoption of mandatory measures of the country or region where the overseas recipient is located), 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 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.

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

(3) This Contract is cancelled with the consent of the Parties, but the cancellation of this Contract shall not exempt 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 return or delete the personal information (including all backups) it has received under this Contract in a timely manner, and provide a written statement to the personal information handler. If it is technically impossible to delete the personal information, the processing of personal information other than storage and any necessary measures taken for the security protection, shall cease.

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) Each Party shall assume civil liabilities to the personal information subject for any infringement on the rights of the personal information subject arising from its breach of this Contract, without prejudice to the administrative, criminal or other liabilities that the personal information handler shall assume under the Relevant Laws and Regulations.

(3) Where the Parties assume joint and several liabilities according to the laws, the personal information subject has the right to request either Party or both Parties to assume the liabilities. When the liability assumed by one Party exceeds the liability such Party shall assumed, it shall have the right to claim against the other Party accordingly.

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 formation, validity, performance and interpretation of this Contract and any dispute between the Parties arising from this Contract shall be governed by the Relevant Laws and Regulations of the People's Republic of China.

(3) All notices shall be promptly sent or mailed by electronic mail, cable, telex, facsimile (with a confirmation copy sent by airmail), or registered airmail to Room 203-A, No. 26 Jia Feng Road, Pilot Free Trade Zone, Shanghai, China (to personal information handler); 1501 Page Mill Road, Palo Alto, California 94304 USA (to overseas recipient), or other address for which written notice is given in lieu of such. If a notice or communication under this Contract is sent by registered airmail, it shall be deemed to have been received twenty (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 five (5) working days after it was sent out.

(4) 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 negotiation fails, either party may take Item 1 of the following methods to resolve the dispute (if arbitration is required, please check the box for the chosen the arbitration institution):

1. Arbitration. Submit the dispute to

■ China International Economic and Trade Arbitration Commission

☐ China Maritime Arbitration Commission

☐ Beijing Arbitration Commission (Beijing International Arbitration Center)

☐ Shanghai International Arbitration Center

☐ Other arbitration institutions that are members 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.

(5) 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.

(6) This Contract shall be executed in three (3) originals, and the Parties, the personal information handler and the overseas recipient, shall each hold one (1) original(s), with the equal legal effect.

This Contract is executed at Shanghai, China.

Personal information handler: HP Trading (Shanghai) Co. Ltd.

[MM/DD/2024]

Overseas recipient: HP Inc.

[MM/DD/2024]

Attachment 7

Brazil Standard Contractual Clauses

SECTION I - GENERAL INFORMATION

CLAUSE 1. Identification of the Parties

1.1 By this agreement, the Exporter and the Importer (hereinafter, "Parties"), identified below, have agreed to these standard contractual clauses (hereinafter, "Clauses") approved by the National Data Protection Authority (ANPD), to govern the International Data Transfer described in CLAUSE 2, in accordance with the provisions of the National Legislation.

Name: See Customer's name in the Agreement

Qualification: Controller

Main Address: Same as in the Agreement

E-mail Address:

Contact for the Data Subject:

Other information: (X) Exporter/Controller) ( ) Exporter/processor)

Name: See HP's name in the Agreement

Qualification: Processor

Main Address: See HP's main address in the Agreement

E-mail Address: https://www.hp.com/us-en/privacy/ww-privacy-form.html

Contact for the Data Subject: https://www.hp.com/us-en/privacy/ww-privacy-form.html

Other information: ( ) Exporter/Controller) (X) Exporter/processor)

CLAUSE 2. Object

2.1 This Clauses shall apply to International Transfers of Personal Data between Data Exporters and Data Importers, as described below.

Description of the international data transfer:

Main purposes of the transfer: See Attachment 1

Categories of personal data transferred: See Attachment 1

Period of data storage: See clause 3.1.6 of the DPA

Other information: N/A

CLAUSE 3. Onward Transfers

3.1. The Importer may carry out an Onward Transfer of Personal Data subject to the International Data Transfer governed by these Clauses, in the cases and according to the conditions described below and the provisions of CLAUSE 18.

Main purposes of the transfer: See Attachment 1

Categories of personal data transferred: See Attachment 1

Period of data storage: See clause 3.1.6 of the DPA

Other information: N/A

CLAUSE 4. Responsibilities of the Parties

4.1 Without prejudice to the duty of mutual assistance and the general obligations of the Parties, the Designated Party below, as Controller, shall be responsible for complying with the following obligations set out in these Clauses:

a) Responsible for publishing the document provided in CLAUSE 14;

(X) Exporter ( ) Importer

b) Responsible for responding to requests from Data Subjects dealt with in CLAUSE 15:

(X) Exporter ( ) Importer

c) Responsible for notifying the security incident provided in CLAUSE 16:

(X) Exporter ( ) Importer

4.2. For the purposes of these Clauses, if the Designated Party pursuant to item 4.1. is the Processor, the Controller remains responsible for:

a) compliance with the obligations provided in CLAUSES 14, 15 and 16 and other provisions established in the National Legislation, especially in case of omission or non-compliance with the obligations by the Designated Party;

b) compliance with ANPD's determinations; and

c) guaranteeing the Data Subjects' rights and repairing damages caused, subject to the provisions of Clause 17.

SECTION II – MANDATORY CLAUSES

CLAUSE 5 Purpose

5.1 These Clauses are presented as a mechanism to enable the secure international flow of personal data, establish minimum guarantees and valid conditions for carrying out the International Data Transfer and aim to guarantee the adoption of adequate safeguards for compliance with the principles, the rights of the Data Subject and the data protection regime provided for in National Legislation.

CLAUSE 6. Definitions

6.1 For the purposes of these Clauses, the definitions in art. 5 of LGPD, and art. 3 of the Regulation on the International Transfer of Personal Data shall be considered, without prejudice to other normative acts issued by ANPD. The Parties also agree to consider the terms and their respective meanings as set out below:

a) Processing agents: the controller and the processor;

b) ANPD: National Data Protection Authority;

c) Clauses: the standard contractual clauses approved by ANPD, which are part of SECTIONS I, II and III;

d) Related Contract: contractual instrument signed between the Parties or, at least, between one of them and a third-party, including a Third-Party Controller, which has a common purpose, link or dependency relationship with the contract that governs the International Data Transfer;

e) Controller: Party or third-party ("Third Controller") responsible for decisions regarding the processing of Personal Data;

f) Personal Data: information related to an identified or identifiable natural person;

g) Sensitive Personal Data: personal data on racial or ethnic origin, religious belief, political opinion, affiliation to trade unions or to a religious, philosophical or political organization, data regarding health or sexual life, genetic or biometric data, whenever related to a natural person;

h) Erasure: exclusion of data or dataset from a database, regardless of the procedure used;

i) Exporter: processing agent, located in the national territory or in a foreign country, who transfers personal data to the Importer;

j) Importer: processing agent, located in a foreign country, who receives personal data from the Exporter;

k) National Legislation: set of Brazilian constitutional, legal and regulatory provisions regarding the protection of Personal Data, including the LGPD, the International Data Transfer Regulation and other normative acts issued by ANPD;

l) Arbitration Law: Law No. 9,307, of September 23, 1996;

m) Security Measures: technical and administrative measures able to protect Personal Data from unauthorized access and from accidental or unlawful events of destruction, loss, alteration, communication or dissemination;

n) Research Body: body or entity of the government bodies or associated entities or a non-profit private legal entity legally established under Brazilian laws, having their headquarter and jurisdiction in the Brazilian territory, which includes basic or applied research of historical, scientific, technological or statistical nature in its institutional mission or in its corporate or statutory purposes;

o) Processor: Party or third-party, including a Sub-processor, which processes Personal Data on behalf of the Controller;

p) Designated Party: Party or a Third-Party Controller, under the terms of CLAUSE 4, designated to fulfill specific obligations regarding transparency, Data Subjects' rights and notifying security incidents;

q) Parties: Exporter and Importer;

r) Access Request: request for mandatory compliance, by force of law, regulation or determination of public authority, to grant access to the Personal Data subject to the International Data Transfer governed by these Clauses;

s) Sub-processor: processing agent hired by the Importer, with no link with the Exporter, to process Personal Data after an International Data Transfer;

t) Third-Party Controller: Personal Data Controller who authorizes and provides written instructions for the carrying out of the International Data Transfer between Processors governed by these Clauses, on his behalf;

u) Data Subject: natural person to whom the Personal Data which are subject to the International Data Transfer governed by these Clauses relate;

v) Transfer: processing modality through which a processing agent transmits, shares or provides access to Personal Data to another processing agent;

w) International Data Transfer: transfer of Personal Data to a foreign country or to an international organization which Brazil is a member of; and

x) Onward Transfer: transfer of Personal Data, within the same country or to another country, by an Importer to a third-party, including a Sub-processor, provided that it does not constitute an Access Request.

CLAUSE 7. Applicable legislation and ANPD supervision

7.1 The International Data Transfer subject to these Clauses shall subject to the National Legislation and to the supervision of ANPD, including the power to apply preventive measures and administrative sanctions to both Parties, as appropriate, as well as the power to limit, suspend or prohibit the international transfers arising from this agreement or a Related Contract.

CLAUSE 8. Interpretation

8.1. Any application of these Clauses shall occur in accordance with the following terms:

a) These Clauses shall always be interpreted more favorably to the Data Subject and in accordance with the provisions of the National Legislation;

b) In case of doubt about the meaning of any term in these Clauses, the meaning which is most in line with the National Legislation shall apply;

c) No item in these Clauses, including a Related Agreement and the provisions set forth in SECTION IV, shall be interpreted as limiting or excluding the liability of any of the Parties in relation to obligations set forth in the National Legislation; and

d) Provisions of SECTIONS I and II shall prevail in case of conflict of interpretation with additional clauses and other provisions set forth in SECTIONS III and IV of this agreement or in Related Agreements.

CLAUSE 9. Docking Clause

9.1. By mutual agreement between the Parties, it shall be possible for a processing agent to adhere to these Clauses, either as a Data Exporter or as a Data Importer, by completing and signing a written document, which shall form part of this contract.

9.2 The acceding party shall have the same rights and obligations as the originating parties, according to the position assumed of Exporter or Importer and according to the corresponding category of treatment agent.

CLAUSE 10. General obligations of the Parties

10.1. The Parties undertake to adopt and, when necessary, demonstrate the implementation of effective measures capable of demonstrating observance of and compliance with the provisions of these Clauses and the National Legislation, as well as with the effectiveness of such measures and, in particular:

a) use the Personal Data only for the specific purposes described in CLAUSE 2, with no possibility of subsequent processing incompatible with such purposes, subject to the limitations, guarantees and safeguards provided for in these Clauses;

b) guarantee the compatibility of the processing with the purposes informed to the Data Subject, according to the processing activity context;

c) limit the processing activity to the minimum required for the accomplishment of its purposes, encompassing pertinent, proportional and nonexcessive data in relation to the Personal Data processing purposes;

d) guarantee to the Data Subjects, subject to the provisions of Clause 4:

(d.1) clear, accurate and easily accessible information on the processing activities and the respective processing agents, with due regard for trade and industrial secrecy;

(d.2) facilitated and free of charge consultation on the form and duration of the processing, as well as on the integrity of their Personal Data; and

(d.3) accuracy, clarity, relevance and updating of the Personal Data, according to the necessity and for compliance with the purpose of their processing;

e) adopt the appropriate security measures compatible with the risks involved in the International Data Transfer governed by these Clauses;

f) not to process Personal Data for abusive or unlawful discriminatory purposes;

g) ensure that any person acting under their authority, including subprocessors or any agent who collaborates with them, whether for reward or free of charge, only processes data in compliance with their instructions and with the provisions of these Clauses;

h) keep a record of the Personal Data processing operations of the International Data Transfer governed by these Clauses, and submit the relevant documentation to ANPD, when requested.

CLAUSE 11. Sensitive personal data

11.1. If the International Data Transfer involves Sensitive Personal Data, the Parties shall apply additional safeguards, including specific Security Measures which are proportional to the risks of the processing activity, to the specific nature of the data and to the interests, rights and guarantees to be protected, as described in SECTION III.

CLAUSE 12. Personal data of children and adolescents

12.1. In case the International Data Transfer governed by these Clauses involves Personal Data concerning children and adolescents, the Parties shall implement measures to ensure that the processing is carried

out in their best interest, under the terms of the National Legislation and relevant instruments of international law.

CLAUSE 13. Legal use of data

13.1. The Exporter guarantees that Personal Data has been collected, processed and transferred to the Importer in accordance with the National Legislation.

CLAUSE 14. Transparency

14.1. The Designated Party shall publish, on its website, a document containing easily accessible information written in simple, clear and accurate language on the conduction of the International Data Transfer, including at least information on:

a) the form, duration and specific purpose of the international transfer;

b) the destination country of the transferred data;

c) the Designated Party's identification and contact details;

d) the shared use of data by the Parties and its purpose;

e) the responsibilities of the agents who shall conduct the processing;

f) the Data Subject's rights and the means for exercising them, including an easily accessible channel made available to respond to their requests, and the right to file a petition against the Exporter and the Importer before ANPD; and

g) Onward Transfers, including those relating to recipients and to the purpose of such transfer.

14.2. The document referred to in item 14.1. shall be made available on a specific website page or integrated, in a prominent and easily accessible format, to the Privacy Policy or equivalent document.

14.3. Upon request, the Parties shall make a copy of these Clauses available to the Data Subject free of charge, complying with trade and industrial secrecy.

14.4. All information made available to Data Subjects, under the terms of these Clauses, shall be written in Portuguese.

CLAUSE 15. Rights of the data subject

15.1. The Data subject shall have the right to obtain from the Designated Party, as regards the Personal Data subject to the International Data Transfer governed by these Clauses, at any time, and upon request, under the terms of the National Legislation:

a) confirmation of the existence of processing;

b) access to data;

c) correction of incomplete, inaccurate or outdated data;

d) anonymization, blocking or erasure of unnecessary or excessive data or data processed in noncompliance with these Clauses and the provisions of National Legislation;

e) portability of data to another service or product provider, upon express request, in accordance with ANPD regulations, complying with trade and industrial secrecy;

f) erasure of Personal Data processed under the Data Subject's consent, except for the events provided in CLAUSE 20;

g) information on public and private entities with which the Parties have shared data;

h) information on the possibility of denying consent and on the consequences of the denial;

i) withdrawal of consent through a free of charge and facilitated procedure, remaining ratified the processing activities carried out before the request for elimination;

j) review of decisions taken solely on the basis of automated processing of personal data affecting their interests, including decisions aimed at defining their personal, professional, consumer and credit profile or aspects of their personality; and

k) information on the criteria and procedures adopted for the automated decision.

15.2. Data subject may oppose to the processing based on one of the events of waiver of consent, in case of noncompliance with the provisions of these Clauses or National Legislation.

15.3 The deadline for responding to the requests provided for in this Clause and in item 14.3 is 15 (fifteen) days from the date of the data subject's request, except in the event of a different deadline established in specific ANPD regulations.

15.4. In case the Data Subject's request is directed to the Party not designated as responsible for the obligations set forth in this Clause or in item 14.3., the referred Party shall:

a) inform the Data Subject of the service channel made available by the Designated Party; or

b) forward the request to the Designated Party as early as possible, to enable the response within the period provided in item 15.2.

15.5. The Parties shall immediately inform the Data Processing Agents with whom they have shared data with the correction, deletion, anonymization or blocking of the data, for them to follow the same

procedure, except in cases where this communication is demonstrably impossible or involves a disproportionate effort.

15.6. The Parties shall promote mutual assistance to respond to the Data Subjects' requests.

CLAUSE 16. Security Incident Reporting

16.1. The Designated Party shall notify ANPD and the Data Subject, within 3 (three) working days of the occurrence of a security incident that may entail a relevant risk or damage to the Data Subjects, according to the provisions of National Legislation.

16.2. The Importer must keep a record of security incidents in accordance with National Legislation.

CLAUSE 17. Liability and compensation for damages

17.1. The Party which, when performing Personal Data processing activities, causes patrimonial, moral, individual or collective damage, for violating the provisions of these Clauses and of the National Legislation, shall compensate for it.

17.2. Data Subject may claim compensation for damage caused by any of the Parties as a result of a breach of these Clauses.

17.3. The defense of Data Subjects' interests and rights may be claimed in court, individually or collectively, in accordance with the provisions in relevant legislation regarding the instruments of individual and collective protection.

17.4. The Party acting as Processor shall be jointly and severally liable for damages caused by the processing activities when it fails to comply with these Clauses or when it has not followed the lawful instructions of the Controller, except for the provisions of item 17.6.

17.5. The Controllers directly involved in the processing activities which resulted in damage to the Data Subject shall be jointly and severally liable for these damages, except for the provisions of item 17.6.

17.6. Parties shall not be held liable if they have proven that:

a) they have not carried out the processing of Personal Data attributed to them;

b) although they did carry out the processing of Personal Data attributed to them, there was no violation of these Clauses or National Legislation; or

c) the damage results from the sole fault of the Data Subject or of a third party which is not a recipient of the Onward Transfer or not subcontracted by the Parties.

17.7. Under the terms of the National Legislation, the judge may reverse the burden of proof in favor of the Data Subject whenever, in his judgement, the allegation is credible, there is a lack of sufficient evidence or when the Data Subject would be excessively burdened by the production of evidence.

17.8. Judicial proceedings for compensation for collective damages which intend to establish liability under the terms of this Clause may be collectively conducted in court, with due regard for the provisions in relevant legislation.

17.9. The Party which compensates the damage to the Data Subject shall have a right of recourse against the other responsible parties, to the extent of their participation in the damaging event.

CLAUSE 18. Safeguards for Onward Transfers

18.1. The Importer shall only carry out Onward Transfers of Personal Data subject to the International Data Transfer governed by these Clauses if expressly authorized, in accordance with the terms and conditions described in CLAUSE 3.

18.2. In any case, the Importer:

a) shall ensure that the purpose of the Onward Transfer is compatible with the specific purposes described in CLAUSE 2;

b) shall guarantee, by means of a written contractual instrument, that the safeguards provided in these Clauses shall be ensured by the third-party recipient of the Onward Transfer; and

c) for the purposes of these Clauses, and regarding the Personal Data transferred, shall be considered responsible for any eventual irregularities committed by the third-party recipient of the Onward Transfer.

18.3. The Onward Transfer shall also be carried out based on another valid modality of International Data Transfer provided in National Legislation, regardless of the authorization referred to in CLAUSE 3.

CLAUSE 19. Access Request Notification

19.1 The Importer shall notify the Exporter and the Data Subject of any Access Request related to the Personal Data subject to the International Data Transfer governed by these Clauses, except in the event that notification is prohibited by the law of the country in which the data is processed.

19.2. The Importer shall implement the appropriate legal measures, including legal actions, to protect the rights of the Data Subjects whenever there is adequate legal basis to question the legality of the Access Request and, if applicable, the prohibition of issuing the notification referred to in item 19.1.

19.3. To comply with both the ANPD's and the Exporter's requests, the Importer shall keep a record of Access Requests, including date, requester, purpose of the request, type of data requested, number of requests received, and legal measures implemented.

CLAUSE 20. Termination of processing and erasure of data

20.1. Parties shall erase the personal data subject to the International Data Transfer governed by these Clauses after the ending of their processing, being their storage authorized only for the following purposes:

a) compliance with a legal or regulatory obligation by the Controller;

b) study by a Research Body, guaranteeing, whenever possible, the anonymization of personal data;

c) transfer to a third-party, upon compliance with requirements set forth in these Clauses and in the National Legislation; and

d) exclusive use of the Controller, being the access by a third-party prohibited, and provided data have been anonymized.

20.2. For the purposes of this Clause, processing of personal data shall cease when:

a) the purpose set forth in these Clauses has been achieved;

b) Personal Data are no longer necessary or pertinent to attain the intended specific purpose set forth in these Clauses;

c) at the termination of the treatment period;

d) Data Subject's request is met; and

e) at the order of ANPD, upon violation of the provisions of these Clauses or National Legislation.

CLAUSE 21. Data processing security

21.1. Parties shall implement Security Measures which guarantee sufficient protection of the Personal Data subject to the International Data Transfer governed by these Clauses, even after its termination.

21.2. Parties shall inform, in SECTION III, the Security Measures implemented, considering the nature of the processed information, the specific characteristics and the purpose of the processing, the technology current state and the probability and severity of the risks to the Data Subjects' rights, especially in the case of sensitive personal data and that of children and adolescents.

21.3. The Parties shall make the necessary efforts to implement periodic evaluation and review measures to maintain the appropriate level of data security.

CLAUSE 22. Legislation of country of destination

22.1 The Importer declares that it has not identified any laws or administrative practices of the country receiving the Personal Data that prevent it from fulfilling the obligations assumed in these Clauses.

22.2. In the event of a regulatory change which alters this situation, the Importer shall immediately notify the Exporter to assess the continuity of the contract.

CLAUSE 23. Non-compliance with the Clauses by the Importer

23.1. In the event of a breach in the safeguards and guarantees provided in these Clauses or being the Importer unable to comply with any of them, the Exporter shall be immediately notified, subject to the provisions in item 19.1.

23.2. Upon receiving the communication referred to in item 23.1 or upon verification of non-compliance with these Clauses by the Importer, the Exporter shall implement the relevant measures to ensure the protection of the Data Subjects' rights and the compliance of the International Data Transfer with the National Legislation and these Clauses, and may, as appropriate:

a) suspend the International Data Transfer;

b) request the return of the Personal Data, its transfer to a third-party, or its erasure; and

c) terminate the contract.

CLAUSE 24. Choice of forum and jurisdiction

24.1. Brazilian legislation applies to these Clauses and any controversy between the Parties arising from these Clauses shall be resolved before the competent courts in Brazil, observing, if applicable, the forum chosen by the Parties in Section IV.

24.2. Data Subjects may file lawsuits against the Exporter or the Importer, as they choose, before the competent courts in Brazil, including those in their place of residence.

24.3. By mutual agreement, Parties may use arbitration to resolve conflicts arising from these Clauses, provided that the procedure is carried out in Brazil and in accordance with the provisions of the Arbitration Law.

SECTION III – Security Measures

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's Information Security program is designed to direct and maintain the organization's information security strategy and controls. This system ensures enterprise-wide compliance with HP's security policies and controls, as well as adherence to the security requirements of its customers. Structured in alignment with industry-standard cybersecurity frameworks, laws, and regulations, the Framework is reviewed annually to adapt to HP's evolving thread landscape.

3. Cybersecurity Risk Management

HP's cybersecurity risk management program is designed to preserve the confidentiality, integrity, and availability of its information assets. The program provides a consistent approach to identifying, assessing, prioritizing, treating, remedying, tracking, and reporting cybersecurity risks. HP defines its Risk Appetite as the acceptable level of loss exposure and Risk Tolerance as the degree of variance from this appetite. Risks are evaluated using a defined methodology, enabling HP to mitigate information security risks to an acceptable level. This program aligns with HP's Enterprise Risk Management process.

4. HR Security

HP Human Resource Security policy ensures information security throughout the employee lifecycle by establishing processes for access to facilities, information systems, and other assets. This includes obtaining written acknowledgments through confidentiality and non-disclosure agreements, as well as conducting background screening procedures. All candidates for employment with HP must complete a background verification check in accordance with relevant laws, regulations, and ethics.

5. Asset Management

HP has a process for identifying technical information assets, categorizing critical assets, and maintaining documented handling procedures for each information classification type, including those containing Personal Data. These procedures cover storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification. HP security policies and standards also mandate the secure disposal of media.

6. Data Security

HP's Data Security program outlines the security practices and technical controls that must be implemented to protect the confidentiality, authenticity, and integrity of data. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification are a few of the factors that determine how information is classified under HP's Data Security policy. In addition to data handling procedures, the policy outlines data encryption, deletion, collection and processing, retention, backup, and data loss prevention.

7. Access Control

HP employs the principle of least privilege for logical access control, providing user access through unique user IDs and passwords. The password policy defines complexity, strength, validity, and password-history controls. Access rights are periodically reviewed and revoked upon personnel departure. Agreed-upon procedures for user account creation and deletion are implemented to grant and revoke access to client systems during engagements.

8. 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. Our Cryptography program involves the use of mathematical techniques to secure information and communications, ensuring that only authorized parties can access the data. A critical component of HP's information security program is protecting data from unauthorized access and tampering.

9. Physical and Environmental Security

HP facilities are secured using various physical and electronic access controls, including security guards, electronic access control, and closed-circuit television (CCTV). Facilities are also equipped with necessary infrastructure support, including temperature control and power backups, using UPS and/or diesel generators to support critical services. All HP personnel are registered and required to carry appropriate identification badges.

10. Operations Management

HP has established minimum hardening requirements for technology infrastructure, including workstations, servers, and network equipment. These devices use pre-hardened operating system images, with requirements varying by operating system and implemented controls. Additionally, HP has deployed Network Intrusion Detection/Prevention Systems (NIDS/NIPS) that are monitored and managed 24/7.

11. Communications Security

Communications Security ensures the protection of information within corporate networks. This includes the installation and management of network security components (e.g., firewalls), segregation of networks, as well as web filtering and email handling controls. Additionally, it involves monitoring and managing communication channels to detect and prevent unauthorized access or data breaches.

12. Systems Security

HP's policy mandates a secure development methodology for systems and software throughout their lifecycle. The Software Development Lifecycle covers initiation, development/acquisition, implementation, operations, and disposal. All system components are evaluated for their impact on overall security. HP has established controls for application service transactions, including user credential validation, digital signatures, encryption, secure communication protocols, and storing transaction details within the appropriate network security zone. Regular internal vulnerability scans are also performed.

13. Third Parties and Subcontractors

HP has processes in place to select sub-contractors who comply with comprehensive contractual security requirements. For applicable suppliers handling HP or customer data, or accessing the HP network, HP Cybersecurity conducts a risk assessment to verify an information security program with physical, technical, and administrative safeguards. This assessment is required before the supplier can access HP information.

14. Information Security Incident Management

HP has a comprehensive Cyber Incident Management Process that outlines purpose, scope, roles, responsibilities, management commitment, organizational coordination, implementation procedures, and compliance checking. This process is reviewed and updated annually. The Cyber Incident Response Team, including HP Cybersecurity personnel trained in incident response and crisis management, conducts regular tabletop reviews of the process and any incidents or events.

15. Business Continuity Management

HP's global Continuity of Operations program ensures end-to-end continuity through collaborative, standardized, and documented planning processes. The company periodically exercises its business continuity plans to ensure effectiveness, testing and updating all plans at least yearly. Additionally, all personnel involved in the business continuity plan receive proper training.

16. Compliance

Compliance shapes HP's approach to meeting legal, contractual, and internal expectations for an effective information security program. Regular information security reviews ensure protocols are integrated into each business group's operations. The review process also keeps documents updated to reflect current legal obligations as requirements evolve.

17. Payment Card Industry

The Payment Card Industry (PCI) framework guides HP's approach to achieving PCI Compliance, outlining business responsibilities and security controls aligned with PCI DSS. By installing and maintaining network security controls like firewalls, HP ensures it meets PCI Compliance requirements.

18. HP Product Security

HP Product Security encompasses essential practices to secure HP Products, such as code signing, managing product security vulnerabilities, issuing security bulletins, and reporting product security issues. These measures ensure that HP products remain secure and reliable for users. Product security is of paramount importance at HP, as it helps maintain customer trust and protects against potential threats.

19. HP Service Security

HP Service Security encompasses essential practices to secure the services provided to HP customers. This policy addresses various areas of service security, including HP infrastructure hosted, third-party hosted, partner hosted, and customer hosted environments. These measures ensure that HP services remain

secure and reliable for users. By implementing robust security practices, HP ensures the safety and integrity of its products and services, fostering a secure and trustworthy environment for all users.

Place and date.

Signatures.

Attachment 8

Saudi Arabia Standard Contractual Clauses (Data Controller to Data Processor)

1.Processing Instructions

The Personal Data Importer shall only process the transferred Personal Data based on written instructions from the Personal Data Exporter. Accordingly, if the Personal Data Importer is unable to follow the instructions, it shall inform the Personal Data Exporter in writing without undue delay.

2.Processing Restrictions

The Personal Data Importer shall process the transferred Personal Data in accordance with the purposes specified in Appendix (2), unless otherwise directed in writing by the Personal Data Exporter, provided that the Personal Data shall be processed in accordance with the provisions of the Law and its Implementing Regulations in all cases.

3.Compliance with the Requests of the Competent Authority

A. In order for the Competent Authority to exercise its powers under the Law and the Implementing Regulations, the parties shall provide a copy of these Clauses to the Competent Authority upon request and without undue delay. The Competent Authority may request any additional information in relation to transfers of Personal Data.

B. Each party agrees to comply with any requests made by the Competent Authority in relation to these Clauses or the processing of the Transferred Personal Data.

C. Upon request, the Personal Data Importer (either directly or through the Personal Data Exporter) shall disclose its identity and contact details and the categories of Personal Data being processed to the Personal Data Subject and provide a copy of these items.

4.Accuracy and Quality of Personal Data

If The Personal Data Importer realizes that any Personal Data transferred is inaccurate or not up-to-date, it shall inform the Personal Data Exporter in writing without undue delay, in which case the Personal Data Importer shall destroy the Personal Data and notify the Personal Data Exporter accordingly, unless the Personal Data Exporter is instructed not to destroy the data because it wishes to correct the transferred Personal Data.

5.Duration of Personal Data Processing and Destruction or Recovery

A. The processing shall be carried out by the Personal Data Importer only for the period specified in Appendix (2). After completion of the purpose of the processing, The Personal Data Importer shall destroy all Personal Data processed on behalf of the Personal Data Exporter and notify the Personal Data Exporter accordingly unless otherwise instructed by the Personal Data Exporter in the following cases:

1. Return all processed Personal Data to the Personal Data Exporter and delete the copies held by the Data Importer;

2. If the applicable regulations in the Kingdom require the retention of the transferred Personal Data for an additional period of time;

B. The Personal Data Importer remains bound by these Clauses until the Personal Data is deleted or recovered.

6.Personal Data Security and Personal Data Breach Notifications

A. The Parties shall ensure that the organizational, administrative, and technical measures specified in Appendix (3) provide a sufficient level of protection for the transferred Personal Data to comply with the requirements of Article (19) of the Law and Article (23) of the Implementing Regulation.

B. The Personal Data Importer shall implement the security measures specified in Appendix (3) and apply those measures to all transferred Personal Data to ensure the security and protection of Personal Data against any violation that may result in damage to the Personal Data Subject, unlawful action, loss, alteration, disclosure, or unauthorized access to Personal Data.

C. The Personal Data Importer must periodically review the security measures stipulated in Appendix (3) to ensure that they are implemented as required and update them as needed to ensure compliance with Article (19) of the Law and Article (23) of the Implementing Regulation.

D. If The Personal Data Importer becomes aware of a Personal Data Breach incident that affects the transferred Personal Data or is likely to cause damage to the rights and interests of Personal Data Subjects, the Personal Data Importer must immediately take appropriate and necessary measures to contain the incident to minimize any risks or negative consequences and ensure that it is prevented from reoccurring. The Personal Data Exporter must be notified within (24) hours from the time of occurrence or knowledge of the breach incident, provided that the notification includes a description of the incident, its causes, the measures taken or planned to be taken to contain the incident and prevent its reoccurrence, in addition to the contact details for follow-up by the Personal Data Exporter. If the Personal Data Exporter realizes that the incident may cause damage to Personal Data or Personal Data Subjects or contradict their rights or interests, it shall notify the Competent Authority within (48) hours and in accordance with the requirements set out in Article (24) of the Law's Implementing Regulation.

E. As soon as the Personal Data Exporter receives the Data Importer's notification of a Personal Data breach incident and the incident would harm the Personal Data or the Personal Data Subject or contradict his/her rights or interests, the Personal Data Exporter must provide immediate notification in simple and

clear language in accordance with the provisions of Article (24) of the Implementing Regulation to the Personal Data Subjects affected by the data breach incident, provided that the notification includes the potential risks and their nature, the measures taken or planned to be taken to contain the incident, and the contact information of the Personal Data Exporter, Data Importer, and the respective Personal Data Protection Officer of both entities, along with recommendations or consultations to aid the Data Subject in preventing or minimizing the impact of the outlined risks.

7.Sensitive Data

Without prejudice to any restrictions related to sensitive data stipulated in the Law and the Implementing Regulations of the Law, the Personal Data Exporter shall ensure that the Personal Data Importer adopts additional means of protection commensurate with the nature of the sensitive data and guarantees its protection from any risks when processing it, while ensuring that the restrictions and additional guarantees described in Appendix (2) are applied.

8.Subsequent Transfer

A. The Personal Data Importer shall not transfer or disclose the transferred Personal Data to a third party outside the Kingdom unless that party has acceded to these Clauses and in accordance with the appropriate template and the provisions of Clause (7) above.

B. Without prejudice to the provisions of Articles (8) and (15) of the Law and (17) of the Implementing Regulation of the Law, the provisions of the Law and Regulations shall apply to Personal Data that has been previously transferred or disclosed to an entity outside the Kingdom.

9.Compliance with these Clauses

A. The Personal Data Importer shall respond to all inquiries of the Personal Data Exporter within the specified period and provide all information requested by the Personal Data Exporter, in addition to providing the Personal Data Exporter with all information it may request regarding the processing of the transferred Personal Data, including any information necessary to enable the Personal Data Exporter to prove its compliance with the requirements contained in these Clauses or the provisions stipulated in the Law and its Implementing Regulations.

B. Each party shall be responsible for demonstrating to the Competent Authority, upon request, that all obligations under these Clauses have been fulfilled.

C. The Personal Data Importer allows the Personal Data Exporter or its appointed representatives to audit the Data Importer's processing of Personal Data without undue delay upon Personal Data Exporter's request.

D. The Personal Data Exporter must provide the information revealed by the audit when requested by the Competent Authority

E. The right of audit does not grant the Personal Data Exporter or its representatives access to any confidential information of the Personal Data Importer as long as this information is not closely related to the processing of the transferred Personal Data.

10. Rights of Personal Data Subjects

A. The Personal Data Importer shall notify the Personal Data Exporter within (48) hours from the time of receipt of the request of any request received from the Personal Data Subject, and the Personal Data Importer shall not have the right to respond to such requests unless the Personal Data Exporter authorizes it to do so.

B. The Personal Data Importer shall take all necessary measures in cooperation with the Personal Data Exporter to respond to the requests of Personal Data Subjects and enable them to exercise their rights under the provisions of the Law and Regulations.

C. The Personal Data Importer is obligated to follow all instructions issued by the Personal Data Exporter regarding the processing of the transferred Personal Data.

D. All statements made to the Personal Data Subject must be presented in a clear, legible, and accessible format.

Attachment 9

Saudi Arabia Standard Contractual Clauses (Data Processor to Data Processor)

1. Instructions Processing.

A. The Personal Data Exporter has clarified to the Personal Data Importer that it processes Personal Data as a Processor based on the instructions of, and on behalf of, its Controller. The Personal Data Exporter confirms that these instructions are compatible and consistent with the instructions provided to it by the Controller.

B. The Personal Data Importer is obliged to process the transferred Personal Data only upon written instructions from the Personal Data Exporter. The Personal Data Importer is obliged to inform the Personal Data Exporter if it is unable to follow these instructions without undue delay.

C. The Personal Data Importer shall notify the Personal Data Exporter if it is unable to comply with The Personal Data Exporter's instructions within (24) hours from the time it becomes aware of this, provided that the Personal Data Exporter shall notify the Controller within (48) hours from the time it receives the Data Importer's notification.

D. The Personal Data Exporter confirms that it has imposed obligations on the Personal Data Importer equivalent to those imposed on the Personal Data Exporter by the Controller with respect to the processing of transferred Personal Data.

2. Processing Restrictions

The Personal Data Importer shall process the transferred Personal Data in accordance with the purposes specified in Appendix (2), unless otherwise directed in writing by the Personal Data Exporter, provided that the Personal Data shall be processed in accordance with the provisions of the Law and its Implementing Regulations in all cases.

3. Compliance with the Requests of the Competent Authority

A. In order for the Competent Authority to exercise its powers under the Law and the Implementing Regulations, the parties shall provide a copy of these Clauses to the Competent Authority upon request and without undue delay. The Competent Authority may request any additional information regarding transfers of Personal Data.

B. Each party agrees to comply with any requests made by the Competent Authority in relation to these Clauses or the processing of the transferred data.

C. Upon request, the Personal Data Importer (either directly or through the Personal Data Exporter or the Controller) shall disclose its identity, contact information, and the categories of Personal Data being processed to the Personal Data Subject and provide a copy of these Clauses.

4. Accuracy and Quality of Personal Data

If The Personal Data Importer realizes that any transferred Personal Data is inaccurate or not up-to-date, it shall inform the Personal Data Exporter in writing without undue delay, provided that the Personal Data Exporter shall inform the Controller within (48) hours from the time the Personal Data Importer notifies the Personal Data Exporter to request a written directive requesting the destruction or correction of the Personal Data.

5. Duration of Personal Data Processing and Destruction or Recovery

A. The processing shall be carried out by the Personal Data Importer only for the period specified in Appendix (2). After completion of the purpose of the processing, the Personal Data Importer shall destroy all Personal Data processed on behalf of the Personal Data Exporter and notify the Personal Data Exporter accordingly, unless otherwise directed by the Personal Data Exporter in the following cases:

1. Return all processed Personal Data to the Personal Data Exporter and delete the copies held by the Data Importer;

2. If the regulations in force in the Kingdom require the retention of the transferred Personal Data for an additional period of time;

3. To retain the minimum amount of Personal Data necessary for the establishment, prosecution, or defense of legal proceedings;

4. Retain the minimum amount of transferred Personal Data necessary to protect the Data Subject's life or vital interests or to prevent, examine, or treat an infection.

B. The Personal Data Importer remains bound by these Clauses until the Personal Data is deleted or recovered.

6. Personal Data Security and Personal Data Breach Notifications

A. The Parties shall ensure that the organizational, administrative, and technical measures specified in Appendix (3) provide a sufficient level of protection for the transferred Personal Data to comply with the requirements of Article (19) of the Law and Article (23) of the Regulation.

B. The Personal Data Importer shall implement the security measures specified in Appendix (3) and apply those measures to all transferred Personal Data to ensure the security and protection of Personal Data against any violation that may result in damage to the Personal Data Subject, unlawful action, loss, alteration, disclosure, or unauthorized access.

C. The Personal Data Importer must periodically review the security measures stipulated in Appendix (3) to ensure that they are being implemented as required, and update them as needed to ensure compliance with Article (19) of the Law and Article (23) of the Regulation.

If Personal Data Importer becomes aware of a data breach incident that could harm the transferred personal data or the data subjects, or conflict with their rights or interests, the Personal Data Importer must immediately take appropriate and necessary measures to contain the incident to minimize any risks or negative consequences and ensure that it does not recur. The Personal Data Exporter must be notified within 24 hours of the breach or upon becoming aware of it. This notification shall include a description of the incident, its causes, the measures taken or planned to contain the incident and prevent its recurrence, and contact details for follow-up by the Personal Data Exporter. The Personal Data Exporter must notify the controller within 24 hours of receiving the notification from the Data Importer. The controller must then notify the competent authority in accordance with the requirements set forth in "Article 24" of the Implementing Regulations of the Law.

7. Sensitive Data

Without prejudice to any restrictions related to sensitive data as stipulated in the Law and its Implementing Regulations, the Personal Data Exporter must ensure that the Data Exporter adopts additional protection measures appropriate to the nature of the sensitive data and ensures its protection from any risks during processing, while also ensuring the application of the restrictions and additional safeguards outlined in Appendix (2).

8. Subsequent Transfer

A. The Data Importer shall not transfer or disclose the transferred Personal Data to a third party outside the Kingdom unless that party has acceded to these Clauses and in accordance with the appropriate template and the provisions of Clause (7) above.

B. Without prejudice to the provisions of Articles (8) and (15) of the Law and (17) of the Implementing Regulation of the Law, the provisions of the Law and Regulations shall apply to Personal Data that has been previously transferred or disclosed to an entity outside the Kingdom.

C. The Controller shall be responsible for verifying that the Personal Data Exporter and Data Importer comply with the above obligations, and the

Controller may appoint an independent third party to review and verify compliance on its behalf. In all cases, if the Personal Data Exporter and Data Importer violate the instructions issued by the Controller or the agreement concluded with it regarding the processing of the transferred Personal Data, the Personal Data Exporter and Data Importer shall be considered as the Controller and shall be responsible for violating the Standard Contractual Clauses and the provisions of the Law and the Implementing Regulations before the Competent Authority.

9. Sub-Processor Appointment

A. If there is a need for the Personal Data Importer to appoint a Sub-Processor, the Personal Data Exporter is required to obtain prior written consent from the Controller at least [specify time period] before appointing any SubProcessor.

B. If a Sub-Processor is appointed, this shall be done through a written agreement that imposes the same obligations as on the Personal Data Importer under these Standard Contractual Clauses. the Personal Data Importer shall, at the request of the Personal Data Exporter, provide a copy of this written agreement and any subsequent amendments thereto to the Personal Data Exporter.

10. Compliance with These Clauses

A. The Personal Data Importer shall respond to all inquiries and requests of the Personal Data Exporter or the Controller within the specified period and provide all information requested by the Personal Data Exporter and Controller, in addition to providing the Personal Data Exporter or the Controller with all information it may request regarding the processing of the transferred Personal Data, including any information necessary to enable the Controller to prove its compliance with the requirements contained in these Clauses or the provisions stipulated in the Law and its Implementing Regulations before the Competent Authority.

B. Each party is responsible for proving that all obligations under these Clauses have been fulfilled before the Competent Authority upon request, and in all cases, if the Personal Data Exporter and Data Importer violate the instructions issued by the Controller or the agreement concluded with it regarding the processing of the transferred Personal Data, the Personal Data Exporter and Data Importer shall be considered as the Controller and shall be responsible for the violation of the Standard Contractual Clauses and the provisions of the Law and the Implementing Regulations before the Competent Authority.

C. The Personal Data Importer shall allow, without undue delay, the Personal Data Exporter or the Controller or their appointed representatives to audit the Data Importer's processing of Personal Data at the request of the Personal Data Exporter or the Controller.

D. The Controller must provide the information revealed by the audit when requested by the Competent Authority.

E. The right of audit does not grant the Personal Data Exporter or the Controller or their representative's access to any confidential information of The Personal Data Importer as long as this information is not closely related to the processing of the transferred Personal Data.

11.Rights of Personal Data Subjects

A. The Personal Data Importer shall notify the Personal Data Exporter within (24) hours of receipt of any request received from the Personal Data Subject, provided that the Personal Data Exporter shall notify the Controller within (24) hours of receipt of the Data Importer's notification, provided that the Personal Data

Importer and the Personal Data Exporter shall not respond to the request unless the Controller authorizes it to do so.

B. The Personal Data Importer shall take all necessary measures, in cooperation with The Personal Data Exporter and the Controller, to respond to the requests of Personal Data Subjects to exercise their rights under the provisions of the Law and Regulations.

C. The Personal Data Importer is obliged to follow all instructions issued by the Personal Data Exporter and the Controller in all matters relating to the processing of the transferred Personal Data.

D. All statements made to the Personal Data Subject must be presented in a clear, legible, and accessible format.