MOBILEIRON, INC.
Programme de protection des données
(Version du 15 mai 2018)

Ce programme de protection des données, y compris les Annexes (collectivement, le « **PPD** »), s'ajoute au Contrat de client conclu entre et par le Client et MobileIron (le « **Contrat** »), il y est incorporé et en fait partie intégrante. En cas de conflit entre une disposition de ce PPD et une disposition du Contrat, la disposition du PPD prévaudra.

1. Définitions.

a. Les termes avec des majuscules initiales utilisés dans ce PPD mais non définis dans celui-ci auront la signification qui leur est donnée dans le Contrat.

b. « **Données des clients** » signifie toutes les Données à caractère personnel communiquées à MobileIron pour le compte du Client par le biais de l'emploi des Services en ligne, dont la mesure est déterminée par le Client à sa discrétion absolue.

c. « **Documentation** » désigne les notes de mises à jour, les guides de mise en œuvre ou toutes autres documentations techniques publiées, sous forme écrite et/ou électronique, relatives à une Solution MobileIron fournie ou mise à la disposition du Client par MobileIron.

d. « **Utilisateur final** » désigne une personne qui utilise une Solution MobileIron.

e. « **Solution MobileIron** » désigne soit le Logiciel ou le Produit SaaS, soit les deux.

f. « **Services en ligne** » désigne des services hébergés par MobileIron que le Client achète en vertu du Contrat comme services autonomes ou inclus dans une plateforme ou une application de MobileIron. Les services en ligne n'incluent pas MobileIron Government Cloud, les essais gratuits, tout service de marque distincte qui fonctionne en dehors du contrôle de MobileIron, ou les logiciels et services fournis sous des conditions de licence ou d'abonnement distinctes. Les Services en ligne n'incluent pas le Logiciel, mais ils peuvent inclure tout service hébergé par MobileIron qui est nécessaire au bon fonctionnement du logiciel.

g. « **Commande** » désigne tout ordre d'achat, bordereau de produits ou bon de commande entre le Client et MobileIron (ou un revendeur autorisé de MobileIron, le cas échéant) qui identifie la Solution MobileIron et/ou les services concédés sous licence ou vendus et les éventuels paramètres d'abonnement et de licence applicables (par exemple, le nombre d'abonnements).

h. « **Données à caractère personnel** » désigne toute information soumise aux Services en ligne et concernant (i) une personne physique identifiée ou identifiable et (ii) une entité juridique identifiée ou identifiable lorsque ces informations sont protégées de la même manière que les Données à caractère personnel ou les informations permettant d'identifier une personne en vertu des lois applicables sur la protection des données. Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, en particulier par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne

i. « **Produit SaaS** » désigne les services rendus disponibles par l'accès au logiciel et l'utilisation du logiciel hébergé par ou pour MobileIron, y compris toute la Documentation.

j. « **Incident de sécurité** » désigne tout accès illégal à des Données à caractère personnel stockées sur des équipements de MobileIron ou dans les installations de MobileIron, ou l'accès non autorisé à ces équipements ou installations entraînant la perte, la divulgation ou la modification des Données à caractère personnel.

k. « **Logiciel** » désigne la version code objet des programmes informatiques appartenant à MobileIron et rendus disponibles par MobileIron en vue de téléchargement par le Client (notamment pour emploi en liaison avec tout Produit SaaS), y compris toute Documentation et toutes Mises à jour.

l. « **Sous-traitants** » désigne les autres responsables du traitement des données qui sont utilisés par MobileIron pour traiter les Données à caractère personnel pour le compte du Client. À titre de précision, les installations du centre de données de colocation de MobileIron ne sont pas des sous-traitants.

m. « **Données de support** » désigne toutes les Données à caractère personnel autres que les Données des clients, fournies à MobileIron par ou pour le compte du Client (ou que ce dernier autorise MobileIron à obtenir depuis les services en ligne) par le biais d'un engagement avec MobileIron pour obtenir un soutien technique et/ou des services de consultation pour les Services en ligne ou les Logiciels couverts par le Contrat, dont l'étendue est contrôlée par le Client à sa seule discrétion.

n. « **Terme** » désigne le terme de l'abonnement au Produit SaaS ou de la licence de Logiciel, tel qu'identifié dans la Commande pertinente, à partir du moment où MobileIron rend initialement disponibles les identifiants permettant d'accéder au Produit SaaS et de l'utiliser, ou de télécharger le Logiciel.

o. « **Mises à jour** » désigne toutes les corrections, mises à jour ou mises à niveau, tous les patchs ou toutes autres modifications ou tous ajouts effectués ou apportés par MobileIron à un Logiciel spécifique.

2. Conformité aux lois.

a. MobileIron. MobileIron doit se conformer à toutes les lois et réglementations applicables à sa fourniture des Services en ligne, y compris la loi sur les notifications des violations de sécurité. Tous les incidents de sécurité sont régis par la Section 7. MobileIron n'est pas responsable du respect des lois ou règlements applicables à l'industrie du Client ou au Client qui ne sont généralement pas applicables aux fournisseurs de services informatiques. MobileIron ne détermine pas si les Données des client ou les Données de support incluent des informations soumises à une loi ou à une réglementation spécifique.

b. Client. Le Client doit se conformer à toutes les lois et réglementations applicables à son utilisation des Services en ligne, y compris les lois relatives à la vie privée, aux Données à caractère personnel, aux données biométriques, à la protection des données et à la confidentialité des communications. Le Client est responsable (i) de la mise en œuvre et du maintien des mesures de sécurité et de protection des composants et des configurations de Solution MobileIron que le Client fournit ou contrôle (y compris les appareils inscrits dans une Solution MobileIron) ; (ii) de la détermination du caractère approprié ou non des Services en ligne pour le stockage et le traitement des informations soumises à des lois ou règlements spécifiques ; (iii) de l'utilisation des Services en ligne conformément aux obligations légales et réglementaires du Client, (iv) des divulgations, de l'obtention des consentements, et de la fournture d'un accès, des choix et d'autres droits applicables aux utilisateurs finaux en ce qui concerne le traitement des Données à caractère personnel requis par la loi, les règles ou les règlements applicables ; et (v) de la réponse à toute demande d'un tiers concernant l'utilisation des Services en ligne par le Client. Pour plus de clarté, le Client peut influencer la portée et la manière du traitement de ses Données à caractère personnel par sa propre mise en oeuvre, configuration et utilisation des Services en ligne, y compris toute autre offre de produits ou services par MobileIron et les intégrations de tiers.

3. Utilisation des Données.

a. Données des clients et Données de support. Les Données des clients seront utilisées uniquement pour fournir au Client les Services en ligne (y compris à des fins compatibles) tels que la mise en œuvre et la livraison de la Solution MobileIron et de ses fonctionnalités et services associés, le soutien au Client et l'assistance au Client pour prévenir ou résoudre les problèmes techniques ou associés aux services. Les Données de support seront uniquement utilisées pour fournir au client une assistance (y compris à des fins compatibles), telle que la résolution des problèmes récurrents et les améliorations apportées au support ou aux services en ligne. MobileIron n'utilisera ni les Données des clients, ni les Données de support et n'en tirera aucune information à des fins publicitaires ou commerciales similaires. En ce qui concerne les relations entre les parties, le Client conserve tous les droits, titres et intérêts dans les Données des clients et les Données de support. MobileIron n'acquiert aucun droit sur les Données des clients ou les Données de support, à part les droits que le Client accorde à MobileIron pour fournir les Services en ligne au Client ou pour fournir un support au Client. Ce paragraphe n'affecte pas les droits de MobileIron dans les Solutions de MobileIron achetées par le Client.

b. Données agrégées et anonymisées. MobileIron collecte, analyse et utilise des données agrégées et rendues anonymes, et d'autres informations connexes (telles que l'utilisation de produits ou de fonctionnalités, les paramètres ou métadonnées d'appareils et/ou l'utilisation faite d'applications mobiles), afin de faciliter la réalisation d'études de marché en vertu du droit applicable ainsi que le développement/l'amélioration de produits et des analyses d'utilisation des produits, et afin de fournir des services de support technique et de maintenance. MobileIron peut utiliser, stocker ou divulguer ces données ou documents dérivés de ces informations, si elles ne permettent pas d'identifier une personne ou ne sont pas attribuables à une personne.

4. **Services professionnels et Données connexes**. Les services professionnels ne sont pas des Services en ligne, et les informations fournies à MobileIron dans le cadre d'un engagement de services professionnels sont protégées en vertu des conditions de confidentialité du Contrat. Le reste de ce PPD ne s'aplique pas à de telles informations, sauf les Données à caractère personnel régies par la Section 14 de ce PPD.

5. Non-divulgation des données

a. MobileIron ne divulguera pas les Données de clients ou les Données de support en dehors de MobileIron ou de ses filiales et sociétés affiliées contrôlées, sauf (i) tel qu'indiqué par le Client, (ii) tel que décrit dans le Contrat ou (iii) conformément à la loi.

b. À la réception d'une demande de tiers ou de la demande de Données de clients ou de Données de support, MobileIron avisera le Client dans les plus brefs délais, sauf si la loi l'interdit. MobileIron rejettera la demande sauf si la loi l'oblige à s'y conformer. Si la demande est valide, MobileIron tentera de faire en sorte que le tiers soumette la demande ou la requête directement au Client.

c. MobileIron ne fournira pas à des tiers : (i) un accès direct, indirect, général ou illimité aux Données de clients ou aux Données de support ; (ii) les clés de chiffrement utilisées pour sécuriser les Données de clients ou les Données de support ou la capacité de contourner un tel chiffrement ; ou (iii) l'accès aux Données de clients ou aux Données de support si MobileIron est consciente du fait que les données seront utilisées à d'autres fins que celles indiquées dans la demande du tiers.

6. **Sécurité.** MobileIron s'engage à aider à protéger la sécurité des Données des clients. MobileIron a mis en place, appliquera et suivra les mesures techniques et organisationnelles appropriées destinées à protéger les Données des clients contre tout accès, divulgation, altération, perte ou destruction accidentels, non autorisés ou illicites. À cet égard, MobileIron a mis en place et maintient pour les systèmes informatiques qui hébergent ou communiquent avec les Services en ligne les mesures de sécurité décrites dans le tableau suivant qui, conjointement avec les engagements de sécurité dans le Contrat et sans préjudice des obligations du Client en vertu de la Section 2.b, sont la seule responsabilité de MobileIron en ce qui concerne la sécurité des Données des clients. MobileIron peut mettre à jour ou modifier les mesures de sécurité décrites ci-dessous de temps en temps si une telle mise à jour ou modification n'entraîne pas la dégradation de la sécurité globale.

Catégorie de contrôle de sécurité	Description
1. Gouvernance	a. Attribuer à une personne ou à un groupe de personnes les rôles appropriés pour développer, coordonner, implémenter et gérer les protections administratives, physiques et techniques de MobileIron conçues pour protéger la sécurité, la confidentialité et l'intégrité des Données à caractère personnel b. Utilisation d'un personnel de sécurité suffisamment formé, qualifié et expérimenté pour pouvoir remplir ses fonctions liées à la sécurité de l'information
2. Contrôles de l'accès	a. Identifier le personnel ou les catégories de personnel dont les fonctions et les responsabilités exigent l'accès aux Données à caractère personnel, aux systèmes pertinents et aux locaux de l'organisation. b. Entretenir des contrôles conçus pour limiter l'accès aux Données à caractère personnel, sux systèmes pertinents et aux installations hébergeant les systèmes au personnel autorisé. c. Passer périodiquement en revue les droits d'accès du personnel. d. Entretenir des contrôles d'accès physiques aux locaux contenant les systèmes, y compris en utilisant des cartes d'accès ou des porte-clés délivrés au personel de MobileIron selon les besoins. e. Mettre en oeuvre des politiques imposant la terminaison de l'accès physique et électronique aux Données à caractère personnel et aux systèmes après la résiliation du contrat de travail d'un employé. f. Concevoir des contrôles de l'accès visant à authentifier les utilisateurs et à limiter l'accès aux systèmes. g. Mettre en oeuvre des politiques limitant l'accès aux installations du centre de données hébergeant les systèmes au personnel du centre de données approuvé et au personnel de MobileIron limité et approuvé. h. Entretenir des processus d'authentification de l'accès à double niveau pour les employés de MobileIron ayant des droits d'accès administratifs aux systèmes
3. Évaluation des risques	a. Effectuer des évaluations périodiques des risques conçues pour analyser les risques existants en matière de sécurité de l'information, identifier les nouveaux risques potentiels et évaluer l'efficacité des contrôles de sécurité existants. b. Maintenir des processus d'évaluation des risques conçus pour évaluer la probabilité d'occurrence des risques et les impacts potentiels importants en cas d'incident. c. Documentation des évaluations formelles des risques. d. Passage en revue des évaluations formelles des risques par le personnel d'encadrement approprié.
4. Classification, rétention et suppression des données	a. Maintenir des politiques établissant une classification des données sur la base de leur criticalité et de leur sensibilité. b. Maintenir des politiques établissant des exigences de rétention et de destruction sécurisée des données.
5. Vérifications des antécédents du personnel	Maintenir des politiques exigeant une vérification raisonnable des antécédents de tout nouvel employé qui aura accès à des Données à caractère personnel ou aux systèmes pertinents, sous réserve du droit local.
6. Formation et éducation du personnel	Former régulièrement et périodiquement le personnel sur les contrôles de sécurité de l'information et les politiques qui sont pertinentes à leurs responsabilités dans l'entreprise et en fonction de leurs rôles au sein de l'organisation.
7. Gestion et supervision des fournisseurs	Examiner périodiquement les rapports d'évaluation de sécurité disponibles des fournisseurs hébergeant les sys afin d'évaluer leurs contrôles de sécurité et d'analyser les exceptions énoncées dans ces rapports.
8. Surveillance, détection des intrusions et réponses en cas d'incident	a. Surveiller l'accès, la disponibilité, la capacité et les performances des systèmes, ainsi que les pare-feu, les journaux système et le trafic des serveurs associés, en utilisant divers logiciels et services de surveillance. b. Maintenir une fonctionnalité de détection/prévention des intrusions (IDS/IPS) sur les systèmes situés aux États-Unis et directement accessibles via un équilibreur de charges. c. Maintenir des procédures d'intervention en cas d'incident pour identifier et signaler les incidents de sécurité, et pour intervenir en conséquence. d. Créer une équipe plurisdiciplinaire d'intervention en cas d'incident relatif à la sécurité.

Catégorie de contrôle de sécurité	Description
9. Encodage	a. Encodage des Données à caractère personnel via HTTPS en utilisant SSL lors de la transmission par des applications Web, et encodage minimum de 128 bits pour tous ces types de trafic. b. Les données de production sont encodées et sauvegardées hors site.
10. Murs pare-feu	Maintenir des murs pare-feu pour le matériel et le logiciel afin de protéger les systèmes.
11. Contrôles des changements	a. Attribuer les responsabilités pour la sécurité des systèmes, les modifications apportées aux systèmes et la maintenance. b. Tester, évaluer et autoriser les principaux composants des systèmes avant leur mise en oeuvre.
12. Sécurité physique	Utilisation des installations de colocation et des centres de données gérés hébergeant les systèmes qui emploient : a. de multiples niveaux de sécurité physique, y compris une surveillance intérieure et extérieure 24 heures sur 24, 365 jours par an, et l'indication de tout accès b. alimentations sans interruption (ASI), générateurs et systèmes de refroidissement
13. Administration et disponibilité des systèmes	a. Utilisation du protocole BGP [Border Gateway Protocol] avec au moins deux FAI de premier niveau conçus pour maintenir l'accès à Internet dans les centres de données hébergeant les systèmes. b. Gérer les processus de correction de sécurité pour les systèmes qui documentent les niveaux de correctifs actuels, déterminer la disponibilité des correctifs et établir des processus de test et d'implémentation des correctifs.

7. **Notification des incidents relatifs à la sécurité**

a. Si MobileIron prend connaissance d'un incident de sécurité, MobileIron (i) notifiera rapidement le client de l'incident de sécurité ; (ii) enquêtera sur l'incident de sécurité et fournira au client des informations détaillées sur l'incident de sécurité ; et (iii) prendra des mesures raisonnables pour atténuer les effets et minimiser les dommages résultant de l'incident de sécurité. MobileIron affectera et formera du personnel pour (i) assurer la liaison avec le Client en ce qui concerne les problèmes de sécurité des Données à caractère personnel ; (ii) recevoir une notification de tout incident de sécurité ; (iii) commuiquer une notification de tout Incident de sécurité au Client conformément à la présente Section 7 et aux lois applicables ; et (iv) coordonner la réponse de MobileIron aux incidents de sécurité et les mesures correctives. L'obligation de MobileIron de notifier ou de répondre ne constitue pas une reconnaissance par MobileIron d'une quelconque faute ou responsabilité à l'égard de l'Incident de sécurité.

b. Le Client doit (i) s'assurer que les administrateurs du Client conservent des informations de contact exactes pour chaque Solution MobileIron et (ii) informer rapidement MobileIron de toute utilisation abusive de ses comptes ou de ses identifiants d'authentification ou de tout Incident de sécurité lié aux Services en ligne.

8. **Lieu du traitement des données**. Sauf tel que décrit par ailleurs dans le Contrat, les Données des cients et les Données de support traitées par MobileIron au nom du Client peuvent être transférées, stockées et traitées aux États-Unis ou dans tout autre pays dans lequel MobileIron ou ses sociétés affiliées ou sous-traitants ont des installations. Généralement, MobileIron stocke les Données des clients dans la région disponible qui est (i) sélectionnée par le Client (si disponible pour les Services en ligne) ou (ii) déterminée en fonction des informations de contact fournies par le Client. Si le Client décide, à la seule discrétion du Client, de soumettre les Données du client et les Données de support à MobileIron avec une demande de support technique, MobileIron peut stocker des Données de clients et des Données de support technique limitées à d'autres endroits pour fournir l'assistance demandée par le Client. Le Client mandate MobileIron pour effectuer un tel transfert de Données de clients et Données de support vers un tel pays et pour stocker et traiter les Données des clients et les Données de support afin de pouvoir fournir les Services en ligne.

9. **Rétention des données**. À tout moment pendant le Terme pour les Services en ligne autonomes, le Client aura la possibilité d'accéder aux Données du client stockées dans les Services en ligne et les extraire, lorsque cela est possible. Sauf pour les essais gratuits, MobileIron conservera les Données de clients stockées dans les Services en ligne autonomes pendant au moins 90 jours après l'expiration du Terme ou de l'abonnement ou de la licence associée afin que le Client puisse extraire les données. Après la période de rétention de 90 jours, MobileIron désactivera le compte du Client et supprimera les Données du client.

10. **Personnel de MobileIron**. Le personnel de MobileIron ne traitera pas les Données du client ou les Données de support sans l'autorisation du client. Le personnel de MobileIron est tenu de maintenir la confidentialité des Données du client et des Données de support conformément aux dispositions du présent PPD, et cette obligation continue même après la fin de leurs engagements.

11. **Sous-traitants.** MobileIron peut engager des sous-traitants, y compris les sociétés affiliées de MobileIron, pour des services limités ou auxiliaires en son nom. De tels sous-traitants seront autorisés à obtenir des Données de clients et de support uniquement pour fournir les services que MobileIron leur a demandé de fournir, et il leur sera interdit d'utiliser les Données de clients et de support à d'autres fins. MobileIron assume la responsabilité du respect par ses sous-traitants des obligations de MobileIron prévues dans le Contrat. Les Sections 18 et 19 contiennent des dispositions additionnelles concernant les sous-traitants.

12. **Audits et contrôles de la sécurité des Services en ligne**

a. Audits. Pour les Services en ligne autonomes, MobileIron lancera au moins une fois par an un audit de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques utilisés pour le traitement des Données de clients par un tiers indépendant qualifié, au choix et aux frais de MobileIron. Chaque audit aboutira à la génération d'un rapport d'audit (« **Rapport d'audit** »), qui sera considéré comme une information confidentielle de MobileIron. Le Rapport d'audit divulguera clairement toutes les constatations importantes de l'auditeur. MobileIron fournira de bonne foi des efforts commercialement raisonnables pour corriger (i) les problèmes soulevés dans tout Rapport d'audit qui pourraient raisonnablement avoir un impact négatif sur la capacité de MobileIron à s'acquitter de ses obligations en vertu de la Section 6 du présent PPD et (ii) les déficiences importantes dans les contrôles. Si le Client le demande, MobileIron fournira au Client le Rapport d'audit ou un résumé conçu pour être partagé avec des tiers afin que le Client puisse vérifier la conformité de MobileIron avec les obligations de sécurité en vertu du PPD. Le Rapport d'audit sera soumis aux obligations de non-divulgation et de limitation de distribution de MobileIron et de l'auditeur.

b. Contrôles de la sécurité. Moyennant un préavis raisonnable, chaque année, à moins que la loi n'exige une autre frquence, MobileIron rendra le personnel raisonnablement disponible pour discuter de la conformité de MobileIron avec la Section 6 du présent PPD ou lui donnera accès aux informations ou à la documentation sur les pratiques de sécurité de MobileIron. se rapportent à ce PPD, y compris, sans s'y limiter, l'accès à tout rapport d'évaluation de la sécurité conçu pour être partagé avec des tiers. Ces informations et documents doivent être considérés comme des informations confidentielles de MobileIron.

13. **Termes additionnels pour l'Australie**. Cette Section 13 ne s'applique que si le Client a des utilisateurs finaux en Australie. Les Données à caractère personnel sont collectées, stockées, utilisées et/ou traitées conformément à la loi Australian Privacy Act 1988 (Commonwealth) et aux Australian Privacy Principles. Si le Client n'est pas satisfait du traitement d'une plainte par MobileIron ou n'est pas d'accord avec la résolution proposée par MobileIron, le Client peut déposer une plainte auprès du Commissariat à l'information australien (OAIC) en contactant l'OAIC selon les méthodes indiquées sur son site Web, https://www.oaic.gov.au/. Le Client peut également demander que MobileIron transmette directement les détails de la plainte du Client à l'OAIC.

14. **Termes additionnels pour l'Europe**. Les Sections 14 à 19 de ce PPD (« **Termes additionnels pour l'Europe** ») s'appliquent au traitement des données à caractère personnel des utilisateurs finaux dans l'Espace économique européen (« **EEE** ») ou en Suisse par MobileIron au nom du Client. L'article 28(1), du Règlement général de l'Union européenne sur la protection des données (« **RGPD** ») exige un accord entre un responsable du traitement et un sous-traitant ainsi qu'entre un contactant direct et un sous-traitant selon lequel le traitement sera conduit conformément à des mesures techniques et organisationnelles conformes aux exigences du RGPD et assurant la protection des droits des personnes concernées. Les Termes additionnels pour l'Europe sont destinés à satisfaire cette exigence pour les parties, y compris dans la mesure où MobileIron est un responsable du traimement des données (ou un sous-traitant) pour les Données à caractère personnel soumises par le Client via un engagement de Services professionnels. Termes utilisés mais non définis dans les termes européens supplémentaires, tels que « **violation de données à caractère personnel** », « **traitement** », « **responsable du traitement** », « **sous-traitant** » et « **personne concernée** » auront le sens qui leur est donné à l'Article 4 du RGPD.

15. **Intention des parties**. Les termes du Contrat, y compris les termes additionnels pour l'Europe et les autres dispositions du PPD, constituent un accord de traitement de données. Pour les Services en ligne, MobileIron est un responsable du traitement des données (ou un sous-traitant) agissant pour le compte du Client. En tant que responsable du traitement des données (ou sous-traitant), MobileIron n'agira qu'en appliquant les instructions du Client. Le Contrat et le PPD (y compris les termes et conditions incorporés par référence dans l'un et l'autre), ainsi que l'utilisation et la configuration des fonctionnalités des Services en ligne par le Client, sont les instructions complètes et finales du Client à MobileIron pour le traitement des Données de clients. Toutes les instructions additionnelles ou alternatives doivent être convenues par écrit.

16. **Description du traitement des données**

a. Objet et durée. L'objet du traitement des Données à caractère personnel est la performance des Services en ligne, y compris les services compatibles. La durée du traitement des données correspond au Terme.

b. Nature et objet. La nature et le but du traitement consistent à fournir les Services en ligne tels que la mise en œuvre et la livraison de la Solution MobileIron et de ses services associés, la fourniture de support technique au client, l'assistance au client pour prévenir ou résoudre des problèmes techniques ou de service, comme la résolution des problèmes récurrents et les améliorations apportées au support technique ou aux Services en ligne.

c. Exportateur de données. Le Client est un responsable du traitement de Données à caractère personnel ou un contractant, et c'est l'exportateur des données.

d. Importateur de données. MobileIron est un responsable du traitement de Données à caractère personnel ou un sous-traitant, est c'est l'importateur des données.

e. Personnes concernées. Les catégories de personnes concernées par les Données à caractère personnel sont les représentants du Client et les Utilisateurs finaux, généralement le personnel du Client qui fournit à MobileIron ses Données à caractère personnel en utilisant une Solution MobileIron.

f. Catégories de données. Les types de Données à caractère personnel traitées, qui varient en fonction de la Solution MobileIron et de son utilisation par le Client, peuvent inclure : (i) les coordonnées de base des Utilisateurs finaux pour l'administration des comptes locaux et pour permettre les communications électroniques relatives au contrôle d'accès ou à la gestion des appareils mobiles ; (ii) des informations de base sur les appareils mobiles pour faciliter leur enregistrement et le déploiement, l'exploitation et la maintenance des Solutions MobileIron ; (iii) les noms, adresses e-mail, noms d'utilisateur et autres données personnelles contenus dans les jetons d'authentification et les certificats Single Sign On concernant les demandes d'authentification des Utilisateurs finaux et les réponses à ces demandes, pour prendre en charge l'authentification sécurisée ; et (iv) d'autres données sous forme électronique utilisées par MobileIron dans le cadre de la Solution MobileIron ou soumises par le Client dans le cadre d'un engagement de Services Professionnels.

g. Opérations de traitement. Les données à caractère personnel transférées seront soumises aux activités de traitement de base suivantes : collecter, stocker, récupérer, consulter, utiliser, effacer ou détruire, divulguer par transmission, disséminer ou mettre à disposition les données de l'exportateur de données selon ce qui est nécessaire pour fournir la solution MobileIron conformément aux instructions de l'exportateur de données, y compris les objectifs internes connexes (tels que le contrôle de la qualité, le dépannage, le développement de produits, etc.).

h. Obligations et droits des Clients. Les obligations et les droits des Clients sont énoncés dans le Contrat et dans le PPD.

17. **Transfert de Données de clients et de Données de support**

a. Tous les transferts de Données de clients et de Données de support hors de l'Espace Économique Européen et de la Suisse vers des pays qui n'assurent pas un niveau adéquat de protection des données au sens des lois sur la protection des données sont régis par l'un des mécanismes de transfert suivants, dans l'ordre spécifié : Premièrement, les autocertifications d'application par MobileIron du Bouclier de protection des données UE-É.-U. et Suisse-É.-U. pour les transferts à destination des É.-U., ou, deuxièmement, les clauses types pour le transfert de Données à caractère personnel aux reponsables du traitement des données établis dans des pays tiers approuvés par la Commission européenne de temps en temps, dont la version approuvée en vigueur à l'heure actuelle est exposée dans la décision 2010/87/UE de la Commission européenne du 5 février 2010 et dans l'Annexe A des Termes additionnels pour l'Europe (les « **Clauses contractuelles standard** »). Les Clauses contractuelles standard seront régies par le droit de l'État membre où le Client est établi.

b. MobileIron se conformera aux exigences de la loi applicable en matière de protection des données concernant la collecte, l'utilisation, le transfert, la conservation et tout autre traitement de données à caractère personnel provenant de l'Espace économique européen et de la Suisse. MobileIron s'engage à informer le Client si elle détermine qu'elle ne pourra plus s'acquitter de son obligation de fournir le même niveau de protection que ce qui est requis par le Bouclier de protection.

c. La signature du Contrat par les deux parties inclut la signature des Clauses contractuelles standard. Les Clauses contractuelles standard ne peuvent pas être invoquées pour légitimer l'exportation de données de tout pays nécessitant une approbation réglementaire, à moins que le Client n'ait obtenu une telle approbation réglementaire.

d. Si les Clauses contractuelles standard s'appliquent, (i) le Client s'engage à exercer son droit d'audit en demandant à MobileIron d'exécuter l'audit et l'examen décrits à la Section 12, (ii) si le Client souhaite modifier cette instruction, le Client a le droit de faire ce qui est indiqué dans les Clauses contractuelles standard, suivant toute demande écrite en ce sens et (iii) rien dans cette section ne saurait changer ou modifier les Clauses contractuelles standard ou affecter les droits de l'autorité de contrôle ou des personnes concernées en vertu des Clauses contractuelles standard.

18. **Dispositions du RGPD**. MobileIron prend les engagements prévus aux Sections 18 et 19 en vigueur au plus tard à compter du début de la mise en application du RGPD ou de l'utilisation des Services en ligne par le Client ou de la fourniture de Services professionnels par MobileIron. La Section 18 reproduit, avec de petites modifications à des fins de clarté, les dispositions

contractuelles pertinentes requises des responsables du traitement des données et des sous-traitants par les Articles 28, 32 et 33 du RGPD. Les références aux articles sont indiquées entre crochets.

a. MobileIron n'engagera pas d'autre sous-traitant pour traiter des données sans l'autorisation générale ou spécifique préalable du Client. Dans le cas d'une autorisation écrite générale, MobileIron informera le Client de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, ce qui donnera au Client la possibilité de s'opposer à de tels changements. [28(2)]

b. MobileIron traitera les Données à caractère personnel uniquement sur instructions documentées du Client, y compris en ce qui concerne les transferts de Données à caractère personnel vers un pays tiers ou une organisation internationale, à moins que cela ne soit requis par la législation de l'Union européenne ou des États membres ; dans un tel cas, MobileIron informera le Client de cette obligation légale avant le traitement, à moins que cette loi n'interdise de telles informations pour des motifs importants d'intérêt public. [28(3)]

c. MobileIron veillera à ce que les personnes autorisées à traiter les Données à caractère personnel se soient engagées à respecter la confidentialité ou soient soumises à une obligation légale de confidentialité. [28(3)]

d. MobileIron prendra toutes les mesures requises en vertu de l'Article 32 du RGPD. [28(3)]

e. MobileIron devra respecter les conditions auxquelles il est fait référence dans les sections 18.a et 18.k pour engager un autre sous-traitant.

f. MobileIron prend en compte la nature du traitement, assiste le Client par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour permettre l'exécution de l'obligation du Client de répondre aux demandes d'exercice des droits des personnes concernées selon le Chapitre III du RGPD. [28(3)]

g. MobileIron aidera le Client à respecter les obligations découlant des articles 32 à 36 du RGPD, en tenant compte de la nature du traitement et des informations à la disposition de MobileIron. [28(3)]

h. MobileIron devra, au choix du Client, supprimer ou renvoyer toutes les Données à caractère personnel au Client après la fin de la fourniture de services relatifs au traitement, et supprimer les copies existantes, sauf si la législation de l'Union Européenne ou des États membres exige le stockage des Données à caractère personnel. [28(3)]

i. MobileIron mettra à la disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD et permettre les audits et y contribuer, y compris les inspections, menées par le Client ou un autre auditeur mandaté par le Client. [28(3)]

j. MobileIron informera immédiatement le Client si, à son avis, une instruction contrevient au RGPD ou à d'autres dispositions de protection des données de l'Union européenne ou des États membres. [28(3)]

k. Lorsque MobileIron engage un autre sous-traitant pour exécuter des activités de traitement spécifiques pour le compte du Client, les mêmes obligations en matière de protection des données que celles prévues à l'Article 28 (3) (et reproduites à la Section 18.b-19.j) sont imposées à cet autre sous-traitant par un contrat ou un autre acte juridique en vertu du droit de l'Union européenne ou de l'État membre, en fournissant notamment des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées de sorte que le traitement réponde aux exigences du RGPD. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, MobileIron reste entièrement responsable vis-à-vis du Client de l'exécution des obligations de cet autre sous-traitant. [28(4)]

l. Compte tenu de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que du niveau inégal des risques et de la gravité en liaison avec les droits et libertés des personnes physiques, le Client et MobileIron devront prendre des mesures organisationnelles et techniques appropriées visant à assurer un niveau de sécurité adapté au risque, y compris, le cas échéant : (i) la pseudonymisation et le cryptage des Données à caractère personnel ; (ii) la capacité de garantir la confidentialité, l'intégrité, la disponibilité et la résilience permanentes des systèmes et services de traitement ; (iii) la possibilité de restaurer la disponibilité et l'accès aux Données à caractère personnel en temps opportun en cas d'incident physique ou technique ; et (iv) un processus pour tester et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. [32(1)]

m. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte des risques présentés par le traitement, notamment la destruction accidentelle ou illicite, la perte, la modification, la divulgation non autorisée ou l'accès aux Données à caractère personnel transmises, stockées ou traitées par ailleurs. [32(2)]

n. Le Client et MobileIron prendront des mesures pour s'assurer que toute personne physique agissant sous l'autorité du Client ou de MobileIron qui a accès aux Données à caractère personnel ne les traite pas, sauf sur les instructions du Client, à moins que la législation de l'Union Européenne ou d'un État membre l'exige. [32(4)]

o. MobileIron devra notifier le Client dans les meilleurs délais de toute violation mettant en danger des Données à caractère personnel dont elle aura pu être avertie. [33 (2)] Cette notification doit, au minimum, (i) décrire la nature de la violation de données personnelles, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, et les catégories et le nombre approximatif de Données à caractère personnel affectées ; (ii) communiquer le nom et les coordonnées du délégué à la protection des données ou de tout autre contact susceptible d'obtenir plus d'informations ; (iii) décrire les conséquences probables de la violation de données personnelles ; et iv) décrire les mesures prises ou envisagées

par le responsable du traitement pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures visant à atténuer les effets négatifs possibles. [33(3)]

19. **Termes additionnel du RGPD**. La présente Section 19 fournit plus de détails sur ce que le client peut attendre de MobileIron pour remplir les conditions de la Section 18, ainsi que sur les engagements de MobileIron concernant les Articles 34-36 du RGPD non couverts par ailleurs dans le contrat.

a. Sous-traitants. Le Client consent à l'engagement de Sous-traitants par MobileIron pour le traitement des Données à caractère personnel conformément aux Sections 18.a et 18.k. Une liste des Sous-traitants actuels de MobileIron est disponible sur demande ou elle peut être consultée sur le site Web de MobileIron. Au moins 14 jours avant d'autoriser un nouveau Sous-traitant à accéder à des Données à caractère personnel, MobileIron mettra à jour la liste. Lorsque MobileIron est un responsable du traitement des données, et non un sous-traitant, les dispositions suivantes s'appliquent : (i) Si le Client n'approuve pas un nouveau Sous-traitant, le Client peut résilier tout abonnement pour les services en ligne concernés sans pénalité en fournissant, avant la fin de la période de préavis, un avis écrit de résiliation incluant une explication des motifs de la non-approbation ; (ii) si les Services en ligne concernés font partie d'un ensemble (ou d'un achat unique similaire de plusieurs services), alors toute résiliation s'appliquera à l'ensemble du groupe ; et (iii) à titre de seul et unique recours du Client, MobileIron remboursera au Client tous les frais d'abonnement prépayés non utilisés.

b. Demandes de Personnes concernées. MobileIron mettra à la disposition du Client les Données à caractère personnel de ses personnes concernées et la possibilité de répondre aux demandes de ces personnes afin d'exercer un ou plusieurs de leurs droits conformément au RGPD en tenant compte des fonctionnalités des Services en ligne et au rôle de contractant responsable du traitement de MobileIron. MobileIron se conformera aux demandes raisonnables du Client pour aider le Client à répondre à une telle demande de personnes concernées si le Client ne peut pas répondre en utilisant la fonctionnalité des Services en ligne. Si MobileIron reçoit une demande d'une personne concernée associée au Client pour exercer un ou plusieurs de ses droits dans le cadre du RGPD, MobileIron redirigera la personne concernée pour faire sa demande directement au Client.

c. Contrôles de la sécurité, audits et inspections. Le Rapport d'audit et les autres informations et documentations décrites à la Section 12 sont destinés à prouver la conformité de MobileIron aux mesures techniques et organisationnelles qui protègent les Services en ligne aux fins de la Section 18.i. Sur demande écrite du Client, MobileIron résumera les conditions de traitement des données dans ses contrats avec les Sous-traitants à la disposition du Client. Le Client peut demander par écrit des informations supplémentaires raisonnables concernant la capacité d'un Sous-traitant à exécuter les activités de traitement pertinentes conformément au présent PPD.

d. Évaluations de l'impact de la protection des données. MobileIron fournira, sur demande, au Client les informations raisonnables requises pour satisfaire aux obligations du Client d'effectuer des évaluations d'impact de la protection des données, le cas échéant, en exécution de ses obligations en vertu de la Section 18.g.

20. **Assistance**. Le Client doit faire une demande écrite d'assistance à laquelle il est fait référence dans le présent PPD. MobileIron pourra facturer au Client des frais raisonnables pour fournir une telle assistance, qui devront être indiqués dans un document d'offre accepté par les parties.

MOBILEIRON, INC.
Termes additionnels pour l'Europe
Annexe A : Clauses contractuelles types (sous-traitants)
(Version du 15 mai 2018)

Aux fins de l'article 26, paragraphe 2 de la directive 95/46/CE pour le transfert des données à caractère personnel vers des sous-traitants établis dans des pays tiers qui n'assurent pas un niveau adéquat de protection des données

Client

(ci-après dénommé **l' « exportateur de données »)**

et

MobileIron, Inc.

401 East Middlefield Road, Mountain View, CA 94043, É.-U. (ci-après dénommée **l' « importateur de données »))**

d'autre part, ci-après dénommés individuellement une «**partie**» et collectivement les « **les parties** »,

SONT CONVENUS des clauses contractuelles suivantes (ci-après dénommées «les clauses») afin d'offrir des garanties adéquates concernant la protection de la vie privée et des libertés et droits fondamentaux des personnes lors du transfert, par l'exportateur de données vers l'importateur de données, des données à caractère personnel visées à l'appendice 1.

Clause première
Définitions

Aux sens des clauses:

a) «données à caractère personnel», «catégories particulières de données», «traiter/traitement», «responsable du traitement», «sous-traitant», «personne concernée» et «autorité de contrôle» ont la même signification que dans la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative 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];

b) l'«exportateur de données» est le responsable du traitement qui transfère les données à caractère personnel;

c) l'«importateur de données» est le sous-traitant qui accepte de recevoir de l'exportateur de données des données à caractère personnel destinées à être traitées pour le compte de ce dernier après le transfert conformément à ses instructions et aux termes des présentes clauses et qui n'est pas soumis au mécanisme d'un pays tiers assurant une protection adéquate au sens de l'article 25, paragraphe 1, de la directive 95/46/CE;

d) le «sous-traitant ultérieur» est le sous-traitant engagé par l'importateur de données ou par tout autre sous-traitant ultérieur de celui-ci, qui accepte de recevoir de l'importateur de données ou de tout autre sous-traitant ultérieur de celui-ci des données à caractère personnel exclusivement destinées à des activités de traitement à effectuer pour le compte de l'exportateur de données après le transfert conformément aux instructions de ce dernier, aux conditions énoncées dans les présentes clauses et selon les termes du contrat de sous-traitance écrit;

e) le «droit applicable à la protection des données» est la législation protégeant les libertés et les droits fondamentaux des personnes, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans l'État membre où l'exportateur de données est établi;

f) les «mesures techniques et d'organisation liées à la sécurité» sont les mesures destinées à protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement.

Clause 2
Détails du transfert

Les détails du transfert et, notamment, le cas échéant, les catégories particulières de données à caractère personnel, sont spécifiés dans l'appendice 1 qui fait partie intégrante des présentes clauses.

[1] Les parties peuvent reprendre, dans la présente clause, les définitions et les significations de la directive 95/46/CE si elles estiment qu'il est préférable que le contrat soit autonome.

Clause 3

Clause de bénéficiaire tiers

1. La personne concernée peut faire appliquer contre l'exportateur de données la présente clause, ainsi que la clause 4, points b) à i), la clause 5, points a) à e) et points g) à j), la clause 6, paragraphes 1 et 2, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12 en tant que tiers bénéficiaire.

2. La personne concernée peut faire appliquer contre l'importateur de données la présente clause, ainsi que la clause 5, points a) à e) et g), la clause 6, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12 dans les cas où l'exportateur de données a matériellement disparu ou a cessé d'exister en droit, à moins que l'ensemble de ses obligations juridiques n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, à laquelle reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre laquelle la personne concernée peut donc faire appliquer lesdites clauses.

3. La personne concernée peut faire appliquer contre le sous-traitant ultérieur la présente clause, ainsi que la clause 5, points a) à e) et g), la clause 6, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12, mais uniquement dans les cas où l'exportateur de données et l'importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, à moins que l'ensemble des obligations juridiques de l'exportateur de données n'ait été transféré, par contrat ou par effet de la loi, au successeur légal, auquel reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre lequel la personne concernée peut donc faire appliquer lesdites clauses. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

4. Les parties ne s'opposent pas à ce que la personne concernée soit représentée par une association ou un autre organisme si elle en exprime le souhait et si le droit national l'autorise.

Clause 4

Obligations de l'exportateur de données

L'exportateur de données accepte et garantit ce qui suit:

a) le traitement, y compris le transfert proprement dit des données à caractère personnel, a été et continuera d'être effectué conformément aux dispositions pertinentes du droit applicable à la protection des données (et, le cas échéant, a été notifié aux autorités compétentes de l'État membre dans lequel l'exportateur de données est établi) et n'enfreint pas les dispositions pertinentes dudit État;

b) il a chargé, et chargera pendant toute la durée des services de traitement de données à caractère personnel, l'importateur de données de traiter les données à caractère personnel transférées pour le compte exclusif de l'exportateur de données et conformément au droit applicable à la protection des données et aux présentes clauses;

c) l'importateur de données offrira suffisamment de garanties en ce qui concerne les mesures techniques et d'organisation liées à la sécurité spécifiées dans l'appendice 2 du présent contrat;

d) après l'évaluation des exigences du droit applicable à la protection des données, les mesures de sécurité sont adéquates pour protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement et elles assurent un niveau de sécurité adapté aux risques liés au traitement et à la nature des données à protéger, eu égard au niveau technologique et au coût de mise en œuvre;

e) il veillera au respect des mesures de sécurité;

f) si le transfert porte sur des catégories particulières de données, la personne concernée a été informée ou sera informée avant le transfert ou dès que possible après le transfert que ses données pourraient être transmises à un pays tiers n'offrant pas un niveau de protection adéquat au sens de la directive 95/46/CE;

g) il transmettra toute notification reçue de l'importateur de données ou de tout sous-traitant ultérieur conformément à la clause 5, point b), et à la clause 8, paragraphe 3), à l'autorité de contrôle de la protection des données s'il décide de poursuivre le transfert ou de lever sa suspension;

h) il mettra à la disposition des personnes concernées, si elles le demandent, une copie des présentes clauses, à l'exception de l'appendice 2, et une description sommaire des mesures de sécurité, ainsi qu'une copie de tout contrat de sous-traitance ultérieure ayant été conclu conformément aux présentes clauses, à moins que les clauses ou le contrat ne contienne(nt) des informations commerciales, auquel cas il pourra retirer ces informations;

i) en cas de sous-traitance ultérieure, l'activité de traitement est effectuée conformément à la clause 11 par un sous-traitant ultérieur offrant au moins le même niveau de protection des données à caractère personnel et des droits de la personne concernée que l'importateur de données conformément aux présentes clauses; et

j) il veillera au respect de la clause 4, points a) à i).

Clause 5

Obligations de l'importateur de données[2]

L'importateur de données accepte et garantit ce qui suit:

a) il traitera les données à caractère personnel pour le compte exclusif de l'exportateur de données et conformément aux instructions de ce dernier et aux présentes clauses; s'il est dans l'incapacité de s'y conformer pour quelque raison que ce soit, il accepte d'informer dans les meilleurs délais l'exportateur de données de son incapacité, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat;

b) il n'a aucune raison de croire que la législation le concernant l'empêche de remplir les instructions données par l'exportateur de données et les obligations qui lui incombent conformément au contrat, et si ladite législation fait l'objet d'une modification susceptible d'avoir des conséquences négatives importantes pour les garanties et les obligations offertes par les clauses, il communiquera la modification à l'exportateur de données sans retard après en avoir eu connaissance, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat;

c) il a mis en œuvre les mesures techniques et d'organisation liées à la sécurité spécifiées dans l'appendice 2 avant de traiter les données à caractère personnel transférées;

d) il communiquera sans retard à l'exportateur de données:

   i) toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre, sauf disposition contraire, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière;

   ii) tout accès fortuit ou non autorisé; et

   iii) toute demande reçue directement des personnes concernées sans répondre à cette demande, à moins qu'il n'ait été autorisé à le faire;

e) il traitera rapidement et comme il se doit toutes les demandes de renseignements émanant de l'exportateur de données relatives à son traitement des données à caractère personnel qui font l'objet du transfert et se rangera à l'avis de l'autorité de contrôle en ce qui concerne le traitement des données transférées;

f) à la demande de l'exportateur de données, il soumettra ses moyens de traitement de données à une vérification des activités de traitement couvertes par les présentes clauses qui sera effectuée par l'exportateur de données ou un organe de contrôle composé de membres indépendants possédant les qualifications professionnelles requises, soumis à une obligation de secret et choisis par l'exportateur de données, le cas échéant, avec l'accord de l'autorité de contrôle;

g) il mettra à la disposition de la personne concernée, si elle le demande, une copie des présentes clauses, ou tout contrat de sous-traitance ultérieure existant, à moins que les clauses ou le contrat ne contienne(nt) des informations commerciales, auquel cas il pourra retirer ces informations, à l'exception de l'appendice 2, qui sera remplacé par une description sommaire des mesures de sécurité, lorsque la personne concernée n'est pas en mesure d'obtenir une copie de l'exportateur de données;

h) en cas de sous-traitance ultérieure, il veillera au préalable à informer l'exportateur de données et à obtenir l'accord écrit de ce dernier;

i) les services de traitement fournis par le sous-traitant ultérieur seront conformes à la clause 11;

j) il enverra dans les meilleurs délais une copie de tout accord de sous-traitance ultérieure conclu par lui en vertu des présentes clauses à l'exportateur de données.

Clause 6

Responsabilité

1. Les parties conviennent que toute personne concernée ayant subi un dommage du fait d'un manquement aux obligations visées à la clause 3 ou à la clause 11 par une des parties ou par un sous-traitant ultérieur a le droit d'obtenir de l'exportateur de données réparation du préjudice subi.

2. Si une personne concernée est empêchée d'intenter l'action en réparation visée au paragraphe 1 contre l'exportateur de données pour manquement par l'importateur de données ou par son sous-traitant ultérieur à l'une ou l'autre de ses obligations visées à la clause 3 ou à la clause 11, parce que l'exportateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'importateur de données accepte que la personne concernée puisse déposer une plainte à son encontre comme s'il était l'exportateur de

[2] Les exigences impératives de la législation nationale le concernant et qui ne vont pas au-delà de celles qui sont nécessaires dans une société démocratique pour l'un des intérêts énoncés à l'article 13, paragraphe 1, de la directive 95/46/CE, c'est-à-dire si elles constituent une mesure nécessaire pour sauvegarder la sûreté de l'État; la défense; la sécurité publique; la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas de professions réglementées; un intérêt économique ou financier important d'un État ou la protection de la personne concernée ou des droits et libertés d'autrui, ne vont pas à l'encontre des clauses contractuelles types. Parmi les exemples de ces exigences impératives qui ne vont pas au-delà de celles qui sont nécessaires dans une société démocratique figurent, notamment, les sanctions reconnues sur le plan international, les obligations de déclaration fiscale et les obligations de déclaration de lutte contre le blanchiment des capitaux.

données, à moins que l'ensemble des obligations juridiques de l'exportateur de données n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, contre laquelle la personne concernée peut alors faire valoir ses droits.

L'importateur de données ne peut invoquer un manquement par un sous-traitant ultérieur à ses obligations pour échapper à ses propres responsabilités.

3. Si une personne concernée est empêchée d'intenter l'action visée aux paragraphes 1 et 2 contre l'exportateur de données ou l'importateur de données pour manquement par le sous-traitant ultérieur à l'une ou l'autre de ses obligations visées à la clause 3 ou à la clause 11, parce que l'exportateur de données et l'importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, le sous-traitant ultérieur accepte que la personne concernée puisse déposer une plainte à son encontre en ce qui concerne ses propres activités de traitement conformément aux présentes clauses comme s'il était l'exportateur de données ou l'importateur de données, à moins que l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données n'ait été transféré, par contrat ou par effet de la loi, au successeur légal, contre lequel la personne concernée peut alors faire valoir ses droits. La responsabilité du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

Clause 7

Médiation et juridiction

1. L'importateur de données convient que si, en vertu des clauses, la personne concernée invoque à son encontre le droit du tiers bénéficiaire et/ou demande réparation du préjudice subi, il acceptera la décision de la personne concernée:
   a) de soumettre le litige à la médiation d'une personne indépendante ou, le cas échéant, de l'autorité de contrôle;
   b) de porter le litige devant les tribunaux de l'État membre où l'exportateur de données est établi.

2. Les parties conviennent que le choix effectué par la personne concernée ne remettra pas en cause le droit procédural ou matériel de cette dernière d'obtenir réparation conformément à d'autres dispositions du droit national ou international.

Clause 8

Coopération avec les autorités de contrôle

1. L'exportateur de données convient de déposer une copie du présent contrat auprès de l'autorité de contrôle si celle-ci l'exige ou si ce dépôt est prévu par le droit applicable à la protection des données.

2. Les parties conviennent que l'autorité de contrôle a le droit d'effectuer des vérifications chez l'importateur de données et chez tout sous-traitant ultérieur dans la même mesure et dans les mêmes conditions qu'en cas de vérifications opérées chez l'exportateur de données conformément au droit applicable à la protection des données.

3. L'importateur de données informe l'exportateur de données, dans les meilleurs délais, de l'existence d'une législation le concernant ou concernant tout sous-traitant ultérieur faisant obstacle à ce que des vérifications soient effectuées chez lui ou chez tout sous-traitant ultérieur conformément au paragraphe 2. Dans ce cas, l'exportateur de données a le droit de prendre les mesures prévues par la clause 5, point b).

Clause 9

Droit applicable

Les clauses sont régies par le droit de l'État membre où l'exportateur de données est établi.

Clause 10

Modification du contrat

Les parties s'engagent à ne pas modifier les présentes clauses. Les parties restent libres d'inclure d'autres clauses à caractère commercial qu'elles jugent nécessaires, à condition qu'elles ne contredisent pas les présentes clauses.

Clause 11

Sous-traitance ultérieure

1. L'importateur de données ne sous-traite aucune de ses activités de traitement effectuées pour le compte de l'exportateur de données conformément aux présentes clauses sans l'accord écrit préalable de l'exportateur de données. L'importateur de données ne sous-traite les obligations qui lui incombent conformément aux présentes clauses, avec l'accord de l'exportateur de données, qu'au moyen d'un accord écrit conclu avec le sous-traitant ultérieur, imposant à ce dernier les mêmes obligations que celles qui incombent à l'importateur de données conformément aux présentes clauses.[3] En cas de manquement, par le sous-traitant ultérieur, aux obligations en matière de protection des données qui lui incombent conformément audit accord écrit, l'importateur de données reste pleinement responsable du respect de ces obligations envers l'exportateur de données.

2. Le contrat écrit préalable entre l'importateur de données et le sous-traitant ultérieur prévoit également une clause du tiers bénéficiaire telle qu'énoncée à la clause 3 pour les cas où la personne concernée est empêchée d'intenter l'action en réparation visée à la clause 6,

[3] Cette condition peut être réputée remplie si le sous-traitant ultérieur est cosignataire du contrat conclu entre l'exportateur de données et l'importateur de données conformément à la présente décision.

paragraphe 1, contre l'exportateur de données ou l'importateur de données parce que ceux-ci ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, et que l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données n'a pas été transféré, par contrat ou par effet de la loi, à une autre entité leur ayant succédé. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

3. Les dispositions relatives aux aspects de la sous-traitance ultérieure liés à la protection des données du contrat visé au paragraphe 1 sont régies par le droit de l'État membre où l'exportateur de données est établi, à savoir …

4. L'exportateur de données tient une liste des accords de sous-traitance ultérieure conclus en vertu des présentes clauses et notifiés par l'importateur de données conformément à la clause 5, point j), qui sera mise à jour au moins une fois par an. Cette liste est mise à la disposition de l'autorité de contrôle de la protection des données de l'exportateur de données.

Clause 12

Obligation après la résiliation des services de traitement des données à caractère personnel

1. Les parties conviennent qu'au terme des services de traitement des données, l'importateur de données et le sous-traitant ultérieur restitueront à l'exportateur de données, et à la convenance de celui-ci, l'ensemble des données à caractère personnel transférées ainsi que les copies, ou détruiront l'ensemble de ces données et en apporteront la preuve à l'exportateur de données, à moins que la législation imposée à l'importateur de données ne l'empêche de restituer ou de détruire la totalité ou une partie des données à caractère personnel transférées. Dans ce cas, l'importateur de données garantit qu'il assurera la confidentialité des données à caractère personnel transférées et qu'il ne traitera plus activement ces données.

2. L'importateur de données et le sous-traitant ultérieur garantissent que si l'exportateur de données et/ou l'autorité de contrôle le demandent, ils soumettront leurs moyens de traitement de données à une vérification des mesures visées au paragraphe 1.

ANNEXE 1 AUX CLAUSES CONTRACTUELLES TYPES

La présente Annexe 1 fait partie des Clauses et doit être remplie par les parties.

Exportateur de données : Le Client est l'exportateur des données.

Importateur de données : MobileIron, Inc. est l'importateur des données.

Personnes concernées : Voir la Section 16 du PPD.

Catégories de données : Voir la Section 16 du PPD.

Catégories particulières de données (le cas échéant) : Voir la Section 16 du PPD.

Opérations de traitement : Voir la Section 16 du PPD.

ANNEXE 2 AUX CLAUSES CONTRACTUELLES TYPES

Le présent appendice fait partie des clauses et doit être rempli et signé par les parties.

Description des mesures techniques et d'organisation liées à la sécurité mises en œuvre par l'importateur de données conformément à la clause 4, point d), et à la clause 5, point c) (ou document/législation jointe): Tel que décrit dans la Section 6 du PPD.