

ACCORD RELATIF AU TRAITEMENT DES DONNÉES PIX4D

Dernière modification : novembre 2021

Le présent Accord relatif au traitement des données et ses Annexes (collectivement l'« **ATD** ») est un contrat entre Vous et Pix4D (Pix4D et Vous, constituant chacun une « **Partie** » et collectivement, les « **Parties** »), régissant le traitement des Données Client à caractère personnel par Pix4D en Votre nom dans le cadre du Contrat de Licence Utilisateur Final (le « **CLUF** »). Le présent ATD est incorporé dans le CLUF et en fait partie intégrante.

Pix4D pourra mettre à jour le présent ATD à tout moment. La version disponible sur notre Site pix4d.com/legal est la version actuelle.

Tous les termes dont la première lettre est en majuscule et qui ne sont pas définis dans le présent ATD ont la signification qui leur est donnée dans le CLUF. Afin d'éviter toute ambiguïté, toute mention du CLUF inclut le présent ATD (y compris ses Documents joints et les CCT de l'UE, tels que définis dans le présent document) et, dans la mesure où elles sont applicables, les Conditions générales pour les clients de Pix4D (les « **Conditions générales** ») et toutes les conditions supplémentaires qui y sont annexées et susceptibles de s'appliquer dans le cadre de l'Utilisation d'un Service spécifique (les « **Conditions supplémentaires** »).

TABLE DES MATIÈRES

ATTENDU QUE	3
1. ENTRÉE EN VIGUEUR ET DURÉE DE L'ATD	3
2. CHAMP D'APPLICATION DE LA LOI SUR LA PROTECTION DES DONNÉES	3
3. TRAITEMENT DES DONNÉES ET RÔLES DES PARTIES	3
4. DEMANDES DES PERSONNE CONCERNÉES	5
5. PERSONNEL DE PIX4D	5
6. SOUS-TRAITANTS	5
7. SÉCURITÉ DES DONNÉES	6
8. TRANSFERTS DE DONNÉES VERS DES PAYS NE FIGURANT PAS SUR LA LISTE BLANCHE	6
9. VIOLATIONS DE DONNÉES	8
10. DEMANDES D'ACCÈS AUX DONNÉES DE LA PART DES POUVOIRS PUBLICS	8
11. EXAMEN ET VÉRIFICATION DE LA CONFORMITÉ	9
12. ÉVALUATIONS D'IMPACT ET CONSULTATIONS	9
13. RESTITUTION OU SUPPRESSION DES DONNÉES	9
14. LIMITATION DE RESPONSABILITÉ	9

15. DIVERS	9
16. DROIT APPLICABLE – RÈGLEMENT DES LITIGES	10
17. DISPOSITIONS SUPPLÉMENTAIRES CONCERNANT LES INFORMATIONS À CARACTÈRE PERSONNEL CALIFORNIENNES	10
18. DÉFINITIONS	11

ATTENDU QUE

- A. Les Parties ont conclu le CLUF en vertu des Conditions générales et des Conditions supplémentaires, le cas échéant.
- B. Dans le cadre de l'exécution du CLUF, Pix4D et/ou l'une de ses Filiales peuvent avoir accès aux Données Client à caractère personnel divulguées ou autrement mises à disposition via les Services sous licence en vertu du CLUF par Vous (ou selon Vos instructions) ou par les Utilisateurs autorisés.
- C. Dans la mesure où Pix4D traitera de telles Données Client à caractère personnel en tant que Votre sous-traitant, les Parties souhaitent s'assurer du fait qu'un tel traitement est conforme au Droit applicable sur la protection des données et conviennent d'un certain nombre de conditions applicables audit traitement, comme indiqué dans le présent ATD.

Par conséquent, les Parties conviennent de ce qui suit :

1. ENTRÉE EN VIGUEUR ET DURÉE DE L'ATD

- 1.1. **Entrée en vigueur.** Le présent ATD entrera en vigueur, et remplacera tout accord de traitement des données précédemment applicable, à compter de la Date d'entrée en vigueur des Conditions (telle que définies ci-dessous).
- 1.2. **Durée de l'ATD.** Indépendamment du fait que le CLUF ait été résilié ou ait expiré, le présent ATD (y compris les Clauses P-C, le cas échéant) restera en vigueur jusqu'à ce que Pix4D supprime toutes les Données Client, conformément aux modalités décrites dans le présent ATD, auquel cas le CLUF expirera automatiquement.

2. CHAMP D'APPLICATION DE LA LOI SUR LA PROTECTION DES DONNÉES

- 2.1. **Application des lois sur la protection des données.** Les Parties reconnaissent que le Droit européen sur la protection des données et, le cas échéant, le Droit non européen sur la protection des données, s'appliqueront au traitement des Données Client à caractère personnel par Pix4D.
- 2.2. **Application des dispositions du présent ATD.** Le présent ATD a été rédigé spécifiquement aux fins du Droit européen sur la protection des données, mais il tient également compte, dans la mesure du possible, des exigences non européennes en matière de protection des données, en particulier du CCPA, selon les modalités énoncées en Section 17, dans la mesure où il est applicable. Sauf indication contraire dans le présent ATD, les dispositions du présent ATD s'appliquent indépendamment du fait que le Droit européen sur la protection des données ou le Droit non européen sur la protection des données s'applique au traitement des Données Client à caractère personnel.

3. TRAITEMENT DES DONNÉES ET RÔLES DES PARTIES

- 3.1. **Rôles des Parties.** Dans le cadre du Droit européen sur la protection des données, les Parties reconnaissent et conviennent qu'en ce qui concerne le traitement des Données Client à caractère personnel dans le cadre de l'exécution du CLUF concernant (i) les Utilisateurs autorisés des Services sous licence dont Vous gérez les comptes (et, en particulier, décidez qui a accès à une Organisation donnée et dans quelle mesure) et/ou (ii) tout autre tiers mentionné

dans le Contenu divulgué à ou autrement mis à la disposition de Pix4D via les Services sous licence en vertu du CLUF, Vous êtes le responsable du traitement des données et Pix4D est le sous-traitant agissant en Votre nom.

3.2. **Traitement ultérieur par Pix4D.** Nonobstant la Section 3.1 ci-dessus, Vous acceptez que Pix4D traite les Données à caractère personnel au-delà de son rôle de sous-traitant, c'est-à-dire en tant que responsable du traitement pour ses propres besoins dans les cas suivants :

- (a) En ce qui concerne les Données à caractère personnel des Utilisateurs autorisés des Services sous licence, y compris les données d'utilisation, dans la mesure du nécessaire pour l'exploitation des Services sous licence (par exemple à des fins de facturation), et plus généralement de l'exécution du CLUF ou de l'exercice de ses droits ; spécifiquement, pour les données d'utilisation, dans la mesure où (a) cette utilisation s'effectue à des fins statistiques, analytiques et autres non liées à des individus particuliers, et (b) toute information éventuellement mise à la disposition de tiers (autres que les prestataires de services de Pix4D soumis à une obligation de confidentialité) (i) ne contient pas de données à caractère personnel identifiables des Utilisateurs autorisés et (ii) ne contient pas de données à caractère personnel identifiables Vous concernant ; lorsque les points (a) et (b) ne s'appliquent pas, nous traiterons des données d'utilisation non anonymisées à des fins d'analyse d'utilisation et d'amélioration des produits, uniquement dans la mesure où Vous aurez accepté un tel traitement dans les paramètres de confidentialité de votre Compte personnel.
- (b) En ce qui concerne les Données à caractère personnel de tiers mentionnés dans le Contenu divulgué à ou autrement mis à la disposition de Pix4D par l'intermédiaire des Services sous Licence, pour ses propres besoins en tant que responsable du traitement, dans la mesure où : (a) cette utilisation s'effectue à des fins statistiques, de recherche et développement, de benchmarking et à d'autres fins non liées à des individus particuliers, et (b) toute information éventuellement mise à la disposition de tiers (autres que les prestataires de services de Pix4D soumis à une obligation de confidentialité) ne (i) contient pas de données à caractère personnel identifiables de tiers et (ii) ne contient pas de Données à caractère personnel identifiables Vous concernant.
- (c) Dans tous les cas, à toutes autres fins requises ou autorisées par les lois sur la protection des données et autres lois applicables.

3.3. **Votre conformité et vos instructions à Pix4D.** Vous déclarez et garantissez que (i) Vous avez respecté, et continuerez à respecter, toutes les lois applicables, y compris le Droit sur la protection des données, en ce qui concerne le traitement que vous faites des Données Client à caractère personnel, leur délégation à Pix4D et toutes les instructions de traitement que vous donnez à Pix4D, et (ii) Vous avez fourni, et continuerez à fournir, tous les avertissements et avez obtenu, et continuerez à obtenir, tous les consentements et toutes les autorisations nécessaires en vertu du Droit sur la protection des données, pour que Pix4D traite les Données Client à caractère personnel aux fins décrites dans le CLUF. Vous êtes seul responsable de l'exactitude, de la qualité et de la légalité des Données Client à caractère personnel et des moyens par lesquels vous avez acquis les Données Client à caractère personnel. Sans préjudice du caractère

général de ce qui précède, Vous acceptez d'être responsable du respect de toutes les Lois (y compris le Droit sur la Protection des données) applicables à tout Contenu créé, envoyé ou géré par le biais des Services sous licence en vertu du CLUF. Par la présente, Vous autorisez et mandatez Pix4D qui gèrera et traitera par ses propres moyens les demandes de suppression de Compte d'utilisateur en Votre nom, dans la mesure où (i) ces demandes sont envoyées par l'Utilisateur directement à Pix4D à l'adresse data_protection@pix4d.com ou par d'autres moyens et (ii) l'Utilisateur est l'un de Vos Utilisateurs Autorisés. En pareil cas, Pix4D pourra Vous informer d'une telle demande de suppression de compte dans la mesure où Pix4D le jugera nécessaire. Le CLUF (y compris le présent ATD), ainsi que l'Utilisation que Vous faites des Services sous Licence et la manière dont Vous les avez configurés conformément au CLUF, constituent l'intégralité des instructions que Vous fournissez à Pix4D pour un traitement pertinent des Données Client à caractère personnel, dans la mesure où Vous pouvez fournir des instructions supplémentaires tout au long de la Durée de l'ATD qui sont compatibles avec le CLUF, la nature, l'étendue des fonctionnalités et la légalité de l'usage des Services sous Licence, et dont les coûts Vous incomberont, sauf disposition contraire. Pix4D Vous informera rapidement par écrit si Pix4D apprend ou estime qu'une instruction de traitement de données de Votre part enfreint le Droit européen sur la protection des données.

- 3.4. **Obligations de Pix4D.** Pix4D traitera les Données Client à caractère personnel en vertu du CLUF conformément au Droit applicable sur la Protection des données et à vos instructions légales étayées, conformément aux modalités énoncées en Section 3.2.
- 3.5. **Modalités du traitement.** L'objet du traitement des Données Client à caractère personnel par Pix4D est l'exécution du CLUF. Les types de données à caractère personnel et les catégories de personnes concernées, la fréquence du transfert, la nature du traitement, la finalité du transfert, la période de conservation des données et les modalités de sous-traitance sont précisés plus en détail dans le [Document C \(Description du transfert\)](#) du présent ATD.

4. DEMANDES DES PERSONNES CONCERNÉES

Pendant la Durée de l'ATD, si Pix4D reçoit de la part d'une personne concernée une demande d'exercice de ses droits de personne concernée en vertu du Droit européen sur la protection des données, et concernant les Données Client à caractère personnel, Pix4D : (i) indiquera à la personne concernée de Vous soumettre sa demande, (ii) Vous en informera rapidement, et (iii) ne répondra par ailleurs pas directement à la demande de cette personne concernée, sauf si cela est nécessaire (par exemple pour demander à la personne concernée de vous contacter) ou constitue une obligation légale, sans Votre autorisation préalable. En outre, Pix4D Vous fournira dans la mesure du possible, en tenant compte de la nature du traitement, une assistance supplémentaire raisonnable pour Vous permettre de Vous conformer à vos obligations en matière de protection des données relativement aux droits des personnes concernées en vertu du Droit européen sur la protection des données. Sous réserve d'un accord textuel préalable entre les Parties, Vous acceptez de rembourser à Pix4D les frais et dépenses raisonnables engagés par Pix4D pour Vous assister conformément à la présente Section 4.

5. PERSONNEL DE PIX4D

Pix4D s'assurera que toute personne autorisée par Pix4D à traiter les Données Client à caractère personnel (y compris les membres de son personnel, ses agents et ses sous-traitants) est soumise à une obligation de confidentialité appropriée (qu'il s'agisse d'une obligation contractuelle ou légale) et qu'elle a notamment accepté de ne pas divulguer de Données Client à caractère personnel à un quelconque tiers, ni de traiter ces données dans un autre but que celui d'exécuter les tâches qui lui sont assignées par Pix4D conformément au CLUF, étant en outre entendu et convenu entre les Parties que Pix4D reste responsable de la conduite de tout personnel de Pix4D comme de sa propre conduite.

6. SOUS-TRAITANTS

- 6.1. **Sous-traitants autorisés.** Vous acceptez que Pix4D puisse engager des sous-traitants pour traiter les Données Client à caractère personnel en votre nom. Les sous-traitants actuellement engagés par Pix4D et autorisés par Vous sont (i) les Filiales de Pix4D et (ii) les tiers mentionnés dans la liste des sous-traitants de Pix4D disponible à l'adresse <https://www.pix4d.com/legal>. Vous donnez en outre par la présente une autorisation écrite d'ordre général à Pix4D pour engager tout autre sous-traitant ultérieur conformément à la présente Section 6, afin d'effectuer des activités de traitement spécifiques au nom de Pix4D.
- 6.2. **Possibilité de s'opposer aux changements de sous-traitants.** En vertu du Droit européen sur la protection des données, Pix4D Vous informera de tout changement prévu concernant l'ajout ou le remplacement de tout sous-traitant et Vous aurez la possibilité de vous opposer à un tel changement pour des raisons objectives et raisonnablement justifiables, dans un délai de trente (30) jours après en avoir été informé. Si tel est le cas, Vous aurez la possibilité d'échanger avec Pix4D au sujet de Vos préoccupations, en vue de parvenir à une solution raisonnable du point de vue commercial. Si aucune solution ne peut être trouvée, Pix4D pourra, à sa seule discrétion, ne pas désigner le nouveau sous-traitant, ou bien Vous permettre de résilier le CLUF conformément aux dispositions de résiliation du CLUF, sans engager la responsabilité de Pix4D (mais sans préjudice de toute redevance due par Vous préalablement à la résiliation du CLUF).
- 6.3. **Exigences relatives à l'engagement d'un sous-traitant.** Lors de l'engagement d'un sous-traitant, Pix4D s'assurera du fait que le sous-traitant est lié par des obligations relatives à la confidentialité et à la protection des données au moins aussi strictes que les dispositions du CLUF (y compris le présent ATD), dans la mesure où elles sont applicables à la nature des activités de traitement fournies par ce sous-traitant, étant entendu et convenu que Pix4D restera responsable de la conduite de chacun de ses sous-traitants comme de sa propre conduite.

7. SÉCURITÉ DES DONNÉES

Pix4D mettra en œuvre et maintiendra des mesures techniques et organisationnelles appropriées, conçues pour protéger les Données Client à caractère personnel contre la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés, accidentels ou illégaux, y compris en particulier et *a minima* les mesures énoncées dans le Document D (les « **Mesures de sécurité** »). Les Mesures de sécurité comprennent des mesures destinées à crypter les Données Client à caractère personnel, à assurer la confidentialité,

l'intégrité, la disponibilité et la résilience continues des systèmes et services de Pix4D, à aider à restaurer en temps utile l'accès aux Données Client à caractère personnel après une Violation de données, et à tester régulièrement leur efficacité. Il Vous incombe d'examiner les informations mises à disposition par Pix4D concernant la sécurité des données et de déterminer de manière indépendante si les Mesures de sécurité répondent à vos exigences et à vos obligations légales en vertu du Droit sur la protection des données. Vous reconnaissez que les Mesures de sécurité sont soumises au progrès et au développement technique et que Pix4D peut mettre à jour ou modifier les Mesures de sécurité à tout moment, à condition que de telles mises à jour et modifications n'entraînent pas la dégradation de la sécurité globale des Services sous Licence qui Vous sont fournis.

8. TRANSFERTS DE DONNÉES VERS DES PAYS NE FIGURANT PAS SUR LA LISTE BLANCHE

8.1. **CCT de l'UE.** Les Parties conviennent que Pix4D peut transférer les Données Client à caractère personnel vers des pays ne figurant pas sur la Liste blanche aux fins de l'exécution du CLUF, ou relativement à elle. Lorsque Pix4D Vous transmet (de retour) des Données Client à caractère personnel soumises au Droit européen sur la protection des données, en tant que responsable du traitement, situé dans un pays ne figurant pas sur la Liste blanche, les Parties acceptent d'être liées par le Module 4 (Transfert de sous-traitant à responsable de traitement) des CCT de l'UE présenté dans le Document A (Module 4 (Transfert de sous-traitant à responsable de traitement) des CCT de l'UE) et compilé comme suit (les « **Clauses P-C** »), et de se conformer à lui, y compris toute modification applicable spécifique à un pays donné énoncée dans le Document B (Modifications spécifiques à certains pays des CCT de l'UE) du présent ATD – Pix4D étant « l'exportateur de données » et Vous étant « l'importateur de données » :

- (d) Les Clauses 1-6 ;
- (e) La Clause 7 ne s'applique pas ;
- (f) La Clause 8 avec les dispositions relatives au « Module 4 », y compris le paragraphe d'introduction ;
- (g) La Clause 10 avec les dispositions relatives au « Module 4 » ;
- (h) La Clause 11(a), hormis les dispositions relatives à l'« Option » de la Clause 11(a) ;
- (i) La Clause 12 avec les dispositions relatives au « Module 4 » ; dans la mesure où elle n'entre pas en conflit avec les CCT de l'UE, la responsabilité entre l'importateur de données et l'exportateur de données (mais pas envers les personnes concernées) sera limitée/exclue conformément à la Section 14 du présent ATD ;
- (j) Les Clauses 14-15 avec les dispositions relatives au « Module 4 », dans la mesure où l'exportateur de données combine les données à caractère personnel reçues de la part de l'importateur de données avec les données à caractère personnel collectées par l'exportateur de données dans un pays figurant sur la Liste blanche ;
- (k) La Clause 16 avec les dispositions relatives au « Module 4 » ;

- (l) La Clause 17 avec les dispositions relatives au « Module 4 », le droit français étant le droit convenu par les Parties aux fins de la Clause 17 ;
 - (m) La Clause 18 avec les dispositions relatives au « Module 4 », les tribunaux français étant compétents selon l'accord convenu par les Parties aux fins de la Clause 18.
- 8.2. **Annexes aux CCT de l'UE.** Les Annexes visées par les Clauses P-C sont établies comme suit :
- (a) L'Annexe I.A contient :
 - i. les informations spécifiées dans le CLUF et fournies par Vous dans le Formulaire d'organisation correspondant, Pix4D étant « l'exportateur de données » agissant en tant que « sous-traitant » et Vous étant « l'importateur de données » agissant en tant que « responsable du traitement » ;
 - ii. les coordonnées de l'exportateur de données : les coordonnées de l'exportateur de données sont Pix4D SA, Route de Renens 24, 1008 Prilly, Suisse. L'équipe de protection des données de l'exportateur de données peut être contactée à l'adresse électronique suivante : data_protection@pix4d.com. Le responsable de la protection des données de l'exportateur de données peut être contacté comme suit : Parrot Drones, c/o Mr Victor Vuillard, 174 Quai de Jemmapes, 75010 Paris, France ;
 - iii. les coordonnées de l'importateur de données : les coordonnées de l'importateur de données, y compris les coordonnées de son responsable de la protection des données, sont à la disposition de l'exportateur de données dans le Formulaire d'organisation correspondant (lorsque ces coordonnées ont été fournies par l'importateur de données) et/ou peuvent être sollicitées par l'exportateur de données séparément par la suite dans des cas spécifiques ;
 - iv. les activités décrites dans le Document C (*Description du transfert*) du présent ATD ;
 - v. les Parties conviennent que l'exécution du CLUF par l'importateur de données et l'exportateur de données constitue l'exécution desdites Clauses P-C par les deux Parties à la Date d'entrée en vigueur des Conditions.
 - (b) L'Annexe I.B est constituée de la section pertinente du Document C (*Description du Transfert*) ;
 - (c) L'Annexe II est constituée du Document B (*Mesures techniques et organisationnelles*) du présent ATD.
 - (d) L'Annexe III, le cas échéant, est constituée de la liste des sous-traitants secondaires de Pix4D, disponible sur <https://www.pix4d.com/legal>.
- 8.3. **Évaluation de l'impact du transfert.** Le Client reconnaît qu'à sa connaissance, les transferts prévus de données à caractère personnel de Pix4D (de retour) vers le Client sont autorisés par la loi en vigueur, et que les Parties n'ont aucune raison de penser que les transferts prévus ne sont pas autorisés.
- 8.4. **Indemnisation.** Chacune des Parties indemniserà l'autre Partie en cas de réclamations de tiers dues à un manquement à ses obligations en vertu des

Clauses P-C.

9. VIOLATIONS DE DONNÉES

En cas de constat d'une violation de données, Pix4D devra : (i) Vous notifier sans retard excessif et, dans la mesure du possible, au plus tard quarante-huit (48) heures après avoir pris connaissance de la violation des données, (ii) fournir des informations opportunes concernant la violation des données dès qu'elles sont connues ou selon Vos demandes raisonnables, et (iii) prendre rapidement des mesures raisonnables pour contenir et examiner toute violation des données. La notification ou la réponse de Pix4D à une violation de données en vertu de la présente Section 9 ne doit pas être interprétée comme une reconnaissance par Pix4D de toute faute ou responsabilité relative à la violation de données.

10. DEMANDES D'ACCÈS AUX DONNÉES DE LA PART DES POUVOIRS PUBLICS

En traitant des Données Client à caractère personnel en tant que Votre sous-traitant en vertu du Droit européen sur la protection des données, Pix4D ne fournit pas aux administrations ou pouvoirs publics, y compris les forces de l'ordre, un accès aux comptes Pix4D ou des informations à leur sujet, y compris les données des clients, sauf obligation légale. Les coûts associés à la réponse à une demande obligatoire (que ce soit par le biais d'une assignation à comparaître, d'une ordonnance judiciaire, d'un mandat de perquisition ou d'une autre procédure légale valide) émanant d'une administration ou d'un pouvoir public, y compris les forces de l'ordre, pour accéder à ou obtenir des informations sur un compte Pix4D, y compris les données des clients, appartenant à Vous et/ou aux Utilisateurs autorisés, seront supportés par Vous.

11. EXAMEN ET VÉRIFICATION DE LA CONFORMITÉ

Pix4D Vous fournira toutes les informations raisonnablement nécessaires pour démontrer le respect de ses obligations en vertu du présent ATD, et permettra les audits et y contribuera, y compris les inspections, menées par Vous ou par un auditeur indépendant nommé par Vous pour vérifier le respect par Pix4D de ses obligations en vertu du présent ATD, sous réserve des clauses de confidentialité habituelles. Pix4D peut en outre Vous fournir, gratuitement, de manière non sollicitée ou sur demande, tout rapport d'audit préparé par l'auditeur de Pix4D confirmant la conformité de Pix4D au présent ATD.

12. ÉVALUATIONS D'IMPACT ET CONSULTATIONS

Dans la mesure où le Droit applicable sur la protection des données l'exige, Pix4D fournira, en tenant compte de la nature du traitement et des informations dont Pix4D dispose, toutes les informations raisonnablement demandées concernant les Services sous licence pour Vous permettre de réaliser des évaluations d'impact sur la protection des données ou des consultations préalables avec les autorités de protection des données, comme l'exige le Droit sur la protection des données. Sous réserve d'un accord écrit préalable entre les Parties, Vous acceptez de rembourser à Pix4D les frais et dépenses raisonnables engagés par Pix4D pour Vous assister, conformément à la présente Section 12.

13. RESTITUTION OU SUPPRESSION DES DONNÉES

À la résiliation ou à l'expiration du CLUF, Pix4D devra (selon votre choix) supprimer

(y compris par le biais de l'anonymisation) ou vous retourner toutes les Données Client à caractère personnel (y compris les copies) en sa possession ou sous son contrôle, mais cette exigence ne s'appliquera pas aux cas où Pix4D est légalement tenu de conserver tout ou partie des Données Client à caractère personnel, ou aux Données Client à caractère personnel archivées sur des systèmes de sauvegarde par Pix4D, que Pix4D isolera de manière sécurisée, protégera de tout traitement ultérieur et supprimera enfin conformément aux politiques de suppression de Pix4D, hormis dans la mesure légalement requise.

14. LIMITATION DE RESPONSABILITÉ

À l'exception des circonstances prévues par les Clauses P-C mentionnées dans les Sections 8.1 et 8.2 et à l'exception des éléments expressément convenus dans le présent ATD, la responsabilité de Pix4D, respectivement Votre responsabilité, est exclue dans la mesure légalement permise.

15. DIVERS

15.1. **Modifications.** Toute modification du présent ATD doit être effectuée par écrit et dûment signée par un représentant autorisé de chacune des Parties.

15.2. **Conflits.** En cas de conflit ou d'incohérence entre le présent ATD et le CLUF concernant le traitement des Données Client à caractère personnel, les dispositions des documents suivants prévaudront (par ordre de préséance) : (i) les CCT de l'UE, puis (ii) le présent ATD, et enfin (iii) le CLUF.

15.3. **Divisibilité.** Si une disposition quelconque de l'ATD est jugée inapplicable pour quelque raison que ce soit, elle sera adaptée plutôt qu'annulée, si possible, afin de concrétiser l'intention juridique et économique des Parties dans toute la mesure du possible. En tout état de cause, toutes les autres dispositions de l'ATD resteront valables et applicables dans toute la mesure du possible.

15.4. **Notifications.** Aux fins de toutes les communications écrites entre les Parties, toute notification ou autre communication faite en rapport avec le CLUF doit être effectuée par écrit (la forme électronique étant considérée comme satisfaisante) et doit être envoyée par courrier électronique aux adresses ci-dessous :

À Pix4D : adresse électronique : legal@pix4d.com.

À Vous : à l'adresse électronique enregistrée dans Votre Compte. En cas de changement, il relève de Votre seule responsabilité d'informer Pix4D de vos nouvelles coordonnées. À cet effet, Vous pouvez contacter l'équipe de support de Pix4D par le biais de la page <https://support.pix4d.com> ou mettre à jour Vos coordonnées sur Votre Compte.

En cas d'utilisation, le système de communication électronique utilisé par Pix4D sera la seule preuve du contenu et de l'heure d'expédition et de réception de ces communications électroniques.

15.5. **Coûts.** Chaque Partie supporte ses propres coûts liés au respect du présent ATD, y compris les Clauses P-C, le cas échéant.

16. DROIT APPLICABLE – RÈGLEMENT DES LITIGES

16.1. Droit applicable. Indépendamment du droit applicable au CLUF, le présent ATD est exclusivement régi et interprété conformément au droit matériel de la Suisse, étant entendu que (i) les conventions internationales, y compris la Convention des Nations Unies sur les contrats de vente internationale de marchandises du 11.04.1980 (CVIM) et (ii) les règles suisses de conflit de lois sont expressément exclues de l'application au présent ATD.

16.2. Juridiction et lieu de juridiction. Indépendamment du lieu de juridiction du CLUF, les tribunaux ordinaires de Lausanne, en Suisse, seront exclusivement compétents pour tout litige survenant entre les Parties à la suite de ou en lien avec le présent ATD.

17. DISPOSITIONS SUPPLÉMENTAIRES CONCERNANT LES INFORMATIONS À CARACTÈRE PERSONNEL CALIFORNIENNES

17.1. Portée et applicabilité. La présente Section 17 de l'ATD s'applique en plus des dispositions du présent ATD, dans la mesure où Pix4D traite des Informations à caractère personnel californiennes en vertu du CLUF soumis au CCPA. En cas de conflit ou d'ambiguïté entre la présente Section 17 et d'autres dispositions du présent ATD, la présente Section 17 aura la priorité, mais uniquement dans la mesure où elle est applicable à Pix4D.

17.2. Rôles des Parties. Lors du traitement d'Informations à caractère personnel californiennes conformément à Vos instructions, les Parties reconnaissent et conviennent que Vous êtes une entreprise et que Pix4D est un prestataire de services aux fins du CCPA.

17.3. Responsabilités. Les Parties conviennent que Pix4D traitera les Informations à caractère personnel californiennes en tant que Prestataire de services dans le strict but d'octroyer des licences pour les Services sous licence en vertu du CLUF (l'« **Objectif commercial** ») ou d'une autre manière autorisée par le CCPA.

18. DÉFINITIONS

ATD	Conformément à la définition fournie en première page.
CCPA	Code civil californien Section 1798.100 et seq., également nommée California Consumer Privacy Act, 2018.
CCT de l'UE	Clauses contractuelles types approuvées par la décision de la Commission européenne du 4 juin 2021 [C(2021)3972 final] pour le transfert de données à caractère personnel vers des pays tiers conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, et toute modification apportée à celui-ci.
Clauses P-C	Module 4 (transfert de sous-traitant à responsable de traitement) des CCT de l'UE, compilé et énoncé dans les Sections 8.1 et 8.2 du présent ATD.

CLUF	Conformément à la définition fournie en première page.
CNIL	Commission nationale de l'informatique et des libertés, conformément à la définition de la Section 8.2
Conditions générales	Conformément à la définition fournie en première page.
Conditions supplémentaires	Conformément à la définition fournie en première page.
Consommateur	Conformément à la définition de « Consumer » du CCPA.
Date d'entrée en vigueur des Conditions	Date à laquelle Vous avez accepté le présent ATD, ou à laquelle les Parties en ont convenu d'une autre manière.
Demande d'une personne concernée	Conformément à la définition de la Section 4.
Données Client	Données fournies par ou pour Votre compte ou celui des Utilisateurs finaux via les Services sous licence dans le cadre du Compte.
Données Client à caractère personnel	Données à caractère personnel contenues dans les Données Client, y compris toute catégorie spéciale de données à caractère personnel.
Droit européen sur la protection des données	Selon le cas, (a) le RGPD et toute législation locale, régionale ou nationale mettant en œuvre le RGPD, (b) le RGPD britannique, et (c) la LPD suisse, et, dans chaque cas, toute version nouvelle ou révisée de l'un de ces règlements susceptible d'entrer en vigueur pendant la Durée de l'ATD.
Droit non européen sur la protection des données	Lois sur la protection des données ou la vie privée en vigueur hors de l'EEE, du Royaume-Uni et de la Suisse, y compris, mais sans s'y limiter, le CCPA.
Droit sur la protection des données	Ensemble des lois et réglementations relatives à la protection des données applicables au traitement par Pix4D ou par vous-même des Données Client à caractère personnel en vertu du CLUF, y compris, le cas échéant, le Droit européen sur la protection des données et le Droit non européen sur la protection des données.
Durée de l'ATD	Période allant de la Date d'entrée en vigueur des Conditions jusqu'à la fin de la fourniture par Pix4D des Services sous licence, y compris, le cas échéant, toute période au cours de laquelle la fourniture des Services sous licence peut être suspendue et toute période post-résiliation au cours de laquelle Pix4D peut continuer

à fournir les Services sous licence ou à des fins transitoires.

EEE	Espace économique européen
Entreprise	Conformément à la définition de « Business » du CCPA.
Formulaire d'organisation	Paramètres d'organisation dans Enterprise User Management fournis par Pix4D pour l'enregistrement de Votre Compte.
Informations à caractère personnel californiennes	Données à caractère personnel soumises à la protection du CCPA.
LPD suisse	Loi fédérale suisse sur la protection des données du 19 juin 1992 et Ordonnance suisse relative à la Loi fédérale sur la protection des données du 14 juin 1993, ainsi que, dans chaque cas, toute version nouvelle ou révisée de ces textes susceptible d'entrer en vigueur pendant la Durée de l'ATD.
Mesures de sécurité	Mesures techniques et organisationnelles de sécurité telles que décrites dans le Document D (<i>Mesures de sécurité</i>).
Objectif commercial	Conformément à la définition de la Section 17.3.
Parties	Conformément à la définition fournie en première page.
Pays figurant sur la Liste blanche	Signifie : <ul style="list-style-type: none">- <i>Pour les Données Client à caractère personnel soumises au RGPD</i> : l'EEE ou un pays ou territoire faisant l'objet d'une décision d'adéquation par la Commission européenne en vertu de l'article 45, paragraphe 1 du RGPD ;- <i>Pour les Données Client à caractère personnel soumises au RGPD britannique</i> : le Royaume-Uni ou un pays ou territoire faisant l'objet d'un règlement d'adéquation en vertu de l'article 45, paragraphe 1 du RGPD britannique et de la Section 17A du Data Protection Act de 2018 ; et/ou- <i>Pour les Données Client à caractère personnel soumises à la LPD suisse</i> : la Suisse ou un pays ou territoire (i) inclus dans la liste des États dont la législation assure un niveau de protection adéquat telle que publiée par le Préposé fédéral à la protection des données et à la transparence ou, selon le cas, (ii) faisant l'objet d'une décision d'adéquation du Conseil fédéral suisse en vertu de la LPD suisse.

Personne concernée	Toute personne physique identifiée ou identifiable à laquelle se rapportent des données à caractère personnel.
PPPDT	Préposé fédéral à la protection des données et à la transparence de la Suisse, au sens de la Section 8.2.
Pix4D, Nous, Notre	Pix4D SA, société anonyme suisse, enregistrée en Suisse sous le numéro CHE-207.009.701, ayant son siège social Route de Renens 24, 1008 Prilly, Suisse.
Prestataire de services	Conformément à la définition de « Service Provider » du CCPA.
Responsable du traitement	Personne physique ou morale, administration publique, agence ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel.
RGPD	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, et abrogeant la Directive 95/46/CE, et toute version nouvelle ou révisée de ce Règlement pouvant entrer en vigueur pendant la Durée de l'ATD.
RGPD britannique	RGPD de l'UE tel que modifié et intégré au droit britannique en vertu du UK European Union (Withdrawal) Act de 2018, et de la législation secondaire applicable adoptée en vertu de cette loi, ainsi que toute version nouvelle ou révisée susceptible d'entrer en vigueur pendant la Durée de l'ATD.
Utilisateurs autorisés	Personnes que Vous autorisez à utiliser les Services sous licence conformément au CLUF. Pour plus de clarté, les Utilisateurs autorisés peuvent inclure Vos employés, Vos sociétés affiliées et toute entité extérieure dûment autorisée par Votre administrateur de compte à devenir membres d'une Organisation où Vous agissez en tant que responsable du traitement pour une telle entité extérieure.
Violation de données	Violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des données à caractère personnel transmises, stockées ou traitées de quelque manière que ce soit par Pix4D, y compris, mais sans s'y limiter, toute violation du <u>Document D (Mesures de sécurité)</u> .

Vous, Votre, Vos

Entité juridique disposant d'une licence d'utilisation des Services sous licence en vertu du CLUF pour une utilisation par ses Utilisateurs autorisés.

Les formules « données à caractère personnel », « personne concernée », « traitement », « responsable du traitement » et « sous-traitant » utilisés dans le présent ATD ont la signification qui leur est donnée dans le RGPD, que le Droit européen sur la protection des données ou le Droit non européen sur la protection des données soit applicable ou non.

Pièces jointes :

Document A : Module 4 (transfert de sous-traitant à responsable de traitement) des CCT de l'UE

Document B : Adaptation des CCT de l'UE à différents pays

Document C : Description du transfert

Document D : Mesures de sécurité

Document A : Module 4 (transfert de sous-traitant à responsable de traitement) des CCT de l'UE

SECTION I

Clause 1

Finalité 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) ⁽¹⁾ 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 « l'entité » 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'Avenant 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

¹ Si l'exportateur de données est un sous-traitant soumis au règlement (UE) 2016/679 agissant pour le compte d'une institution ou d'un organe de l'Union en tant que responsable du traitement, le recours aux présentes Clauses lors du recrutement d'un autre sous-traitant (sous-traitance ultérieure) qui n'est pas soumis au règlement (UE) 2016/679 garantit également le respect de l'article 29, paragraphe 4, du règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39), dans la mesure où les présentes clauses et les obligations en matière de protection des données fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément à l'article 29, paragraphe 3, du règlement (UE) 2018/1725 sont alignées. Ce sera en particulier le cas lorsque le responsable du traitement et le sous-traitant se fondent sur les clauses contractuelles types qui figurent dans la décision 2021/915.

ou mettre à jour des informations dans l'Avenant. 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 8.1 (b) et Clause 8.3 (b) ;
 - (iii) N/A
 - (iv) N/A
 - (v) Clause 13 ;
 - (vi) Clause 15.1 (c), (d) et (e) ;
 - (vii) Clause 16 (e) ;
 - (viii) 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

Hierarchie

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'Avenant et en signant l'Annexe I.A.
- (b) Une fois l'Avenant 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 l'ATD.

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 ne traite les données à caractère personnel que sur instructions documentées de l'importateur de données agissant en tant que son responsable du traitement.
- (b) S'il n'est pas en mesure de suivre ces instructions, notamment si elles constituent une violation du règlement (UE) 2016/679 ou d'autres dispositions législatives de l'Union ou d'un État membre en matière de protection des données, l'exportateur de données en informe immédiatement l'importateur de données.
- (c) L'importateur de données s'abstient de tout acte susceptible d'empêcher l'exportateur de données de s'acquitter des obligations qui lui incombent en vertu du règlement (UE) 2016/679, notamment dans le cadre d'une sous-traitance ultérieure ou en ce qui concerne la coopération avec les autorités de contrôle compétentes.
- (d) Au terme de la prestation des services de traitement, l'exportateur de données, à la convenance de l'importateur 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.

8.2 Sécurité du traitement

- (a) Les Parties mettent en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données, notamment pendant la transmission, et 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 (ci-après la « violation de données à caractère

personnel »). Lors de l'évaluation du niveau de sécurité approprié, elles tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre, de la nature des données à caractère personnel ⁽²⁾, 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, et 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.

- (b) L'exportateur de données aide l'importateur de données à garantir une sécurité appropriée des données conformément au paragraphe (a). En cas de violation de données à caractère personnel concernant les données à caractère personnel traitées par l'exportateur de données au titre des présentes Clauses, ce dernier en informe l'importateur de données dans les meilleurs délais après avoir eu connaissance de la violation et l'aide à y remédier.
- (c) L'exportateur de données 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.

8.3 Documentation et conformité

- (a) Les Parties sont en mesure de démontrer le respect des présentes Clauses.
- (b) L'exportateur de données met à la disposition de l'importateur de données toutes les informations nécessaires pour démontrer le respect des obligations qui lui incombent au titre des présentes Clauses et pour permettre la réalisation d'audits et y contribuer.

Clause 9

Recours à des sous-traitants ultérieurs

N/A

Clause 10

Droits des personnes concernées

Les Parties se prêtent mutuellement assistance pour répondre aux demandes de renseignements et aux autres demandes formulées par les personnes concernées en vertu de la législation locale applicable à l'importateur de données ou, en cas de traitement par l'exportateur de données dans l'Union, en vertu du règlement (UE) 2016/679.

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.

² Il s'agit notamment de savoir si le transfert et le traitement ultérieur portent sur 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 ou à des infractions.

[OPTION : L'importateur de données convient que les personnes concernées peuvent également introduire, sans frais, une réclamation auprès d'un organe de règlement des litiges indépendant ⁽³⁾. Il informe les personnes concernées, de la manière indiquée au paragraphe (a), de ce mécanisme de recours et du fait qu'elles ne sont pas tenues d'y recourir ni de respecter une hiérarchie dans les recours.]

Clause 12

Responsabilité

- (a) Chaque Partie est responsable envers la ou les autres Parties de tout dommage qu'elle cause à l'autre ou aux autres Parties du fait d'un manquement aux présentes Clauses.
- (b) Chaque Partie 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 une Partie 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 en vertu du règlement (UE) 2016/679.
- (c) 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.
- (d) Les Parties conviennent que, si la responsabilité d'une d'entre elles est reconnue en vertu du paragraphe (c), celle-ci est en droit de réclamer auprès de l'autre ou des autres Parties la part de la réparation correspondant à sa/leur part de responsabilité dans le dommage.
- (e) L'importateur de données ne peut invoquer le comportement d'un sous-traitant ou d'un sous-traitant ultérieur pour échapper à sa propre responsabilité.

Clause 13

Supervision

N/A

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

(lorsque le sous-traitant de l'UE combine les données à caractère personnel reçues du responsable du traitement du pays tiers et des données à caractère personnel qu'il a collectées dans l'UE)

- (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

³ L'importateur de données ne peut proposer un règlement des litiges indépendant par une instance d'arbitrage que s'il est établi dans un pays qui a ratifié la convention de New York pour la reconnaissance et l'exécution des sentences arbitrales étrangères.

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) les 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) les législations et les 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 les limitations et les garanties applicables ⁽⁴⁾ ;
 - (iii) 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

⁴ 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.

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 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

(lorsque le sous-traitant de l'UE combine les données à caractère personnel reçues du responsable du traitement du pays tiers et des données à caractère personnel qu'il a collectées dans l'UE)

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 (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 (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 (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 collectées par l'exportateur de données dans l'UE qui ont été transférées avant la résiliation du contrat au titre du paragraphe (c), ainsi que toute copie de celles-ci, sont immédiatement effacées dans leur intégralité. 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 pays qui reconnaît des droits au tiers bénéficiaire. Les Parties conviennent qu'il s'agit du droit de _____ (précisez l'État membre).]

Clause 18
Élection de for et juridiction

Tout litige survenant du fait des présentes Clauses est tranché par les juridictions de _____ (précisez l'État membre). **AVENANT**

NOTE EXPLICATIVE :

Il doit être possible de distinguer clairement les informations applicables à chaque transfert ou catégorie de transferts et, à cet égard, de déterminer le ou les rôles respectifs des Parties en tant qu'exportateur(s) et/ou importateur(s) de données. Il n'est pas forcément nécessaire de remplir et de signer des avenants distincts pour chaque transfert/catégorie de transferts et/ou relation contractuelle, si cette transparence peut être garantie au moyen d'un seul avenant. Toutefois, si cela est nécessaire pour garantir une clarté suffisante, il convient d'utiliser des avenants distincts.

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

Document B : Adaptation des CCT de l'UE à différents pays

Suisse

Aux fins de la Loi suisse sur la protection des données (LPD), lorsque les transferts de Données à caractère personnel en vertu du CLUF sont soumis au RGPD et à la LPD suisse, les Clauses P-C applicables conformément aux Sections 8.1 et 8.2 du présent ATD s'appliquent avec les modifications suivantes (pour éviter toute ambiguïté, ces modifications n'affectent pas les Clauses P-C telles qu'applicables aux fins du RGPD) :

- Les références au « Règlement (UE) 2016/679 » ou à « ce Règlement » doivent être interprétées comme des références à la LPD suisse dans la mesure où elle est applicable.
- Les références au « Règlement (UE) 2018/1725 » sont supprimées.
- Les références à « Union », « UE » et « État membre de l'UE » doivent être interprétées comme des références à la Suisse.
- La Clause 17 est remplacée par : « Les présentes Clauses sont régies par le droit suisse dans la mesure où les transferts sont régis par la LPD suisse ».
- La Clause 18 est remplacée par le texte suivant :
« Tout litige découlant des présentes Clauses relatives au DPA suisse sera résolu par les tribunaux suisses. Une personne concernée peut également intenter une action en justice contre l'exportateur et/ou l'importateur de données devant les tribunaux de Suisse dont dépend sa résidence habituelle. Les Parties acceptent de se soumettre à la juridiction de ces tribunaux ».
- Jusqu'à l'entrée en vigueur de la LPD suisse révisée, les Clauses P-C protègent également les données à caractère personnel des personnes morales et ces dernières bénéficient de la même protection en vertu des Clauses P-C que les personnes physiques.

Aux fins de la LPD suisse, lorsque les transferts de Données à caractère personnel en vertu du CLUF sont soumis exclusivement à la LPD suisse, les Clauses P-C applicables conformément aux Sections 8.1 et 8.2 du présent ATD s'appliquent avec les modifications suivantes :

- Les références au « Règlement (UE) 2016/679 » ou à « ce Règlement » doivent être interprétées comme des références à la LPD suisse.
- Les références au « Règlement (UE) 2018/1725 » sont supprimées.
- Les références à « Union », « UE » et « État membre de l'UE » doivent être interprétées comme des références à la Suisse.
- La Clause 17 est remplacée par le texte suivant : « Les présentes Clauses sont régies par le droit suisse ».
- La Clause 18 est remplacée par le texte suivant :
« Tout litige découlant des présentes Clauses relatives à la LPD suisse sera résolu par les tribunaux suisses. Une personne concernée peut également intenter une action en justice contre l'exportateur et/ou l'importateur de données devant les tribunaux de Suisse dont dépend sa résidence habituelle. Les Parties acceptent de se soumettre à la juridiction de ces tribunaux ».

- Jusqu'à l'entrée en vigueur de la LPD suisse révisée, les Clauses P-C protègent également les données à caractère personnel des personnes morales et ces dernières bénéficient de la même protection en vertu des Clauses P-C que les personnes physiques.

Document C : Description du transfert

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

Les Personnes concernées sont les personnes au sujet desquelles des données sont fournies à Pix4D, via les Services sous licence, par Vous (ou selon Vos instructions) ou par les Utilisateurs autorisés, y compris les tiers mentionnés dans le Contenu.

Catégories de données à caractère personnel transférées :

Données relatives à des personnes fournies à Pix4D, via les Services, par Vous (ou selon Vos instructions) ou par les Utilisateurs autorisés, y compris les tiers mentionnés dans le Contenu.

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 :

Les Parties ne prévoient pas le transfert de données sensibles.

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

Régulière et continue.

Nature du traitement :

Pix4D traitera les Données Client à caractère personnel dans le but de fournir les Services sous licence pour une utilisation par Vous et les Utilisateurs autorisés, conformément au CLUF.

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 :

Durée de l'ATD plus période allant de la fin de la Durée de l'ATD à la suppression de toutes les Données Client par Pix4D conformément au CLUF et au présent ATD.

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

Voir la liste des sous-traitants de Pix4D, disponible à l'adresse <https://www.pix4d.com/legal>.

Document D : Mesures de sécurité

Ce qui suit constitue la description des mesures techniques et organisationnelles mises en œuvre par Pix4D (y compris toute certification pertinente) pour assurer un niveau de sécurité approprié (les « **Mesures de sécurité** »), compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes concernées :

1. Mesures de pseudonymisation et de cryptage des données à caractère personnel.
 - a) La pseudonymisation est effectuée de manière à ce qu'aucune donnée ne puisse être associée à une personne concernée spécifique sans informations supplémentaires.
 - b) Les informations supplémentaires permettant d'attribuer des données à caractère personnel à une personne spécifique sont conservées dans des systèmes distincts et sécurisés, uniquement accessibles à un nombre de personnes limité.
 - c) Lors du cryptage des données à caractère personnel, les algorithmes et la longueur des clés sont proportionnés au degré de sensibilité des données.
 - d) Les clés de cryptage sont conservées en toute sécurité et sont uniquement communiquées à un nombre de personnes limité.
 - e) Des instructions internes garantissent que l'anonymisation / la pseudonymisation se poursuit dans la mesure du possible en cas de divulgation ou même après l'expiration du délai légal de suppression.
2. Mesures visant à garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement
 - a) Un responsable de la sécurité ou un membre désigné de la direction générale est nommé pour être chargé de la coordination et du contrôle des règles et procédures de sécurité de l'information.
 - b) La protection des données fait partie intégrante de la gestion des risques de l'entreprise.
 - c) Des plans d'urgence et de contingence sont maintenus pour les installations dans lesquelles se trouvent les systèmes d'information traitant les données à caractère personnel.
 - d) Si nécessaire, une analyse d'impact relative à la protection des données (AIPD) est réalisée.
 - e) Le personnel est formé et tenu à la confidentialité et au secret des données.
 - f) Le personnel est informé des procédures de sécurité pertinentes et du rôle de chacun.
 - g) Le personnel est informé des conséquences possibles du non-respect des règles et procédures de sécurité.
 - h) Des instructions opérationnelles sur le contrôle d'accès, la sécurité des communications et la sécurité opérationnelle sont fournies au personnel.
 - i) Ces instructions opérationnelles décrivent explicitement les mesures de sécurité, les procédures pertinentes et les responsabilités.

- j) Toutes les règles, instructions et directives relatives à la protection des données sont documentées de manière centralisée et accessibles à tous les employés.
 - k) Les composants critiques pour le fonctionnement du système sont surveillés en continu et protégés dans la mesure nécessaire par des systèmes de protection contre le feu, l'eau, l'humidité, les chocs, la chaleur, le froid et les coupures de courant imprévues.
 - l) Les composants critiques pour le fonctionnement du système peuvent être remplacés dans les délais requis en cas de défaillance, par exemple, par des composants de secours, des systèmes RAID ou la mise en miroir des données.
 - m) Si nécessaire, des partitions distinctes sont utilisées pour les systèmes d'exploitation et les données.
3. Mesures visant à garantir la capacité de restaurer la disponibilité et l'accès aux données à caractère personnel en temps utile en cas d'incident physique ou technique
- a) Une stratégie de sauvegarde est définie en fonction de la quantité de données et de leur fréquence de changement.
 - b) La stratégie de sauvegarde est conçue pour retrouver les données à caractère personnel dans l'état où elles étaient avant la perte ou la destruction des données.
 - c) Les systèmes de sauvegarde sont physiquement séparés des systèmes de production.
 - d) Les mesures de sécurité appliquées aux serveurs de sauvegarde et aux serveurs de production sont identiques.
 - e) Les personnes chargées de restaurer les données sont spécialement formées en la matière.
4. Procédures pour tester, évaluer et apprécier régulièrement l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement.
- a) L'efficacité des mesures techniques et organisationnelles (MTO) est testée à intervalles prédéfinis par l'importateur des données. La nature et la fréquence de ces tests sont définies en fonction de la mesure concernée.
 - b) Des mesures appropriées sont définies et engagées si les tests montrent que les MTO ne sont pas ou pas suffisamment mises en œuvre, ou si elles ne présentent pas l'efficacité requise.
 - c) De nouvelles MTO sont introduites si l'examen des MTO existantes indique qu'elles ne sont plus suffisantes (en cas de nouvelles menaces, par exemple).
 - d) Une ou plusieurs personnes sont désignées pour contrôler en continu l'efficacité des MTO et pour coordonner les tests et les éventuelles mesures à prendre.
5. Mesures d'identification et d'autorisation des utilisateurs

- a) L'accès aux systèmes d'information est protégé par des procédures d'identification et d'authentification conformes aux normes industrielles.
 - b) Les dispositifs de stockage de données, les postes de travail, les ordinateurs portables, les smartphones et les tablettes sont chiffrés à l'aide de méthodes de chiffrement conformes aux normes du secteur.
 - c) Les comptes et les autorisations des utilisateurs sont gérés par des personnes désignées (administrateurs).
 - d) Les droits d'accès aux bases de données sont restrictifs, accordés en fonction des besoins et gérés par un nombre minimum d'administrateurs.
 - e) L'accès aux données à caractère personnel est limité aux employés qui ont un besoin légitime d'accéder à ces données dans le cadre de leur fonction ou rôle individuel.
 - f) Les données collectées à des fins différentes peuvent être traitées séparément des autres données.
 - g) Les activités du système au-delà de l'accès autorisé sont empêchées.
 - h) Des directives sont élaborées et mises en œuvre sur les thèmes suivants : « mots de passe sécurisés », « suppression/destruction », « clean desk », « appareil mobile ».
 - i) Tout compte utilisateur permettant l'authentification est individuel et utilisé par une seule personne.
 - j) Le personnel a pour instruction de désactiver les sessions administratives lorsqu'il quitte les locaux ou lorsque les postes de travail sont laissés sans surveillance.
 - k) Les mots de passe des utilisateurs sont composés d'au moins huit caractères, dont des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.
 - l) Une authentification à deux facteurs est utilisée pour accéder aux systèmes critiques.
 - m) L'outil de destruction des fichiers et/ou la destruction externe des fichiers sont conformes à la norme de sécurité DIN 66399.
6. Mesures de protection des données pendant la transmission
- a) L'accès à distance s'effectue uniquement sur des lignes cryptées (VPN).
 - b) Le transfert électronique de données et la transmission de données à caractère personnel s'effectuent à l'aide de méthodes de cryptage conformes aux normes du secteur. Pour les e-mails, le cryptage de ligne (TLS), au moins, est utilisé lorsqu'il est pris en charge.
 - c) Des procédures de signature sont mises en œuvre si nécessaire.
 - d) Les données ne sont pas transférées à des tiers inconnus.
7. Mesures de protection des données pendant leur stockage
- a) L'accès à des données spécifiques est limité aux personnes qui ont besoin de traiter ces données. Cet accès est contrôlé par un modèle d'autorisation des utilisateurs.

- b) Le cas échéant, les différentes données clients sont stockées dans des bases de données différentes.
 - c) Les supports de stockage externes qui contiennent des données à caractère personnel sensibles sont cryptés et physiquement sécurisés.
 - d) Les droits de saisie, de modification et de suppression des données nécessitent une autorisation.
 - e) Les droits d'effacement sont octroyés de manière restrictive.
8. Mesures visant à assurer la sécurité physique des lieux où sont traitées les données à caractère personnel
- a) Les systèmes et services sont protégés contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la divulgation ou l'accès non autorisés.
 - b) Un système d'alarme anti-effraction comprenant une alarme 24/7 est installé.
 - c) Les portes extérieures et intérieures sont sécurisées par des contacts magnétiques de fermeture.
 - d) Les clés et cartes d'accès sont attribuées à des personnes spécifiques.
 - e) L'entrée ou la réception est surveillée à tout moment pendant les heures de travail.
 - f) Les bâtiments et les entrées sont sous surveillance vidéo permanente.
 - g) Les visiteurs sont toujours accompagnés par des employés.
 - h) Le personnel externe est rigoureusement sélectionné.
 - i) Pour les systèmes logés, hébergés et maintenus par des prestataires de services externes, les mesures correspondantes à mettre en œuvre et à maintenir par ces prestataires de services sont organisées.
9. Mesures visant à garantir l'enregistrement des événements
- a) Les autorisations d'accès et la récupération des données sont contrôlées et consignées.
 - b) L'attribution des clés et des cartes d'accès est consignée.
 - c) L'accès des visiteurs est consigné.
 - d) La saisie, la modification et la suppression de données sont consignées.
 - e) Les tentatives de restauration des données sont consignées.
 - f) Les résultats des tests d'efficacité des mesures techniques et organisationnelles sont consignés.
 - g) Les résultats des tests de structure des rapports sont consignés.
 - h) Les incidents de sécurité et les violations de données sont consignés. Des journaux d'événements sont maintenus, qui comprennent la nature de la violation des données, les catégories et le nombre approximatif de personnes concernées, les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés, la période, les conséquences de la violation des données, la procédure de récupération des données, les mesures prises pour atténuer les effets négatifs, le(s)

nom(s) de la (des) personne(s) qui a (ont) signalé la violation des données et le(s) nom(s) de la (des) personne(s) à qui la violation des données a été signalée.

- i) Les journaux permettent la traçabilité des utilisateurs individuels plutôt que des groupes d'utilisateurs.
10. Mesures visant à garantir la configuration des systèmes, y compris la configuration par défaut
- a) Des mesures techniques sont engagées pour permettre aux personnes concernées d'exercer facilement leur droit de retirer leur consentement.
 - b) Des paramètres par défaut respectueux de la protection des données sont utilisés dans les logiciels standards et individuels.
11. Mesures pour la gouvernance et la gestion de l'informatique interne et de la sécurité informatique
- a) Un logiciel antivirus et un pare-feu sont installés sur les serveurs et les clients afin d'éviter que des logiciels malveillants n'accèdent aux systèmes sans autorisation.
 - b) Un système de détection des intrusions est en place.
 - c) Une procédure formalisée de traitement des incidents de sécurité est en place.
 - d) L'accès à distance par des parties externes est surveillé.
 - e) Les matériels et les logiciels informatiques sont vérifiés à intervalles prédéfinis, afin de déterminer s'ils doivent être mis à jour ou remplacés pour des raisons de sécurité.
12. Mesures de certification/assurance des procédures et des produits
- a) Le besoin de certifications pour les systèmes et les produits est régulièrement évalué.
 - b) Les certifications de sécurité des données (le cas échéant) et les audits (y compris les tests de pénétration, le cas échéant) sont régulièrement renouvelés.
13. Mesures visant à garantir la minimisation des données
- a) Les données à caractère personnel sont uniquement collectées dans la mesure où elles sont nécessaires pour atteindre les objectifs prévus.
 - b) Les données à caractère personnel détenues sont révisées périodiquement et supprimées si elles ne sont plus utilisées et si aucune exigence légale ou contractuelle n'interdit la suppression de ces données à caractère personnel.
14. Mesures visant à garantir la qualité des données
- a) Le cas échéant, la saisie des données est soumise à des tests de plausibilité.
 - b) Le cas échéant, les utilisateurs ont la possibilité de vérifier les données saisies.
15. Mesures visant à garantir une conservation limitée des données

- a) Lorsque cela est approprié et possible, des périodes de conservation sont définies.
 - b) Des protocoles d'archivage automatisé sont utilisés pour les documents et les données dans les systèmes productifs, lorsque cela est possible et approprié.
16. Mesures visant à assurer l'imputabilité
- a) Une procédure formalisée est définie pour le suivi des incidents de sécurité et des violations de données.
 - b) Les mécanismes de contrôle relatifs au respect des principes de protection des données sont basés sur les exigences des lois en vigueur en matière de protection des données.
 - c) Les structures de reporting sont alignées sur l'organisation du groupe et de l'unité concernée et permettent de réagir dans un délai raisonnable et, le cas échéant, légal.
 - d) L'efficacité des structures de reporting est testée à intervalles prédéfinis.
 - e) Des mesures appropriées sont définies et prises si les tests montrent que les structures de reporting ne sont pas ou pas suffisamment mises en œuvre ou n'ont pas l'efficacité requise.
17. Mesures destinées à permettre la portabilité des données et à assurer leur effacement
- a) Les responsabilités en matière de portabilité des données sont clairement définies.
 - b) Des procédures formalisées sont en place pour les demandes de portabilité des données.
 - c) Les ensembles de données peuvent être identifiés et triés par les fonctions de sélection du système employé.
 - d) Les demandes de portabilité des données sont envoyées sans délai aux unités adéquates et traitées rapidement, afin que les délais légaux soient respectés en toutes circonstances.
 - e) Des mesures appropriées sont mises en œuvre pour assurer la suppression des données à caractère personnel des systèmes du fournisseur à la fin du contrat principal.
 - f) Les personnes responsables de la portabilité des données sont formées et compétentes sur la manière de traiter les demandes concernant la portabilité des données. En particulier, les informations qui doivent être divulguées, transférées ou supprimées, et les demandes ou parties de ces demandes qui ne doivent pas être satisfaites sont clairement définies.
 - g) Les données à caractère personnel sont transmises en utilisant des formats structurés, couramment utilisés et lisibles par machine, en utilisant des méthodes sécurisées.