

## ACCORD SUR LA CONFIDENTIALITÉ, LA SÉCURITÉ ET LE TRAITEMENT DES DONNÉES (« DPA »)

Le présent DPA est conclu entre le Client identifié dans le Accord de Services par Abonnement (« SSA ») applicable et l'entité Planview identifiée dans le SSA (« Planview ») et régit le traitement par Planview des PII (telles que définies ci-dessous) du Client, sous réserve du SSA.

### 1. Objet du DPA

Aux fins du présent DPA, le terme « PII » désigne les données à caractère personnel, les informations personnelles et/ou les informations personnelles identifiables, telles que définies dans les Lois Applicables sur la Protection des Données identifiées ci-dessous. Planview traite les PII dans le but de fournir au Client divers services décrits dans le SSA (les « Services »). Le présent DPA établit les instructions données par le Client à Planview et les activités de traitement convenues par Planview pour le compte du Client lors du traitement des PII en relation avec les Services. Planview agit en tant que sous-traitant ou prestataire de services, tel que défini dans les Lois Applicables sur la Protection des Données (« Sous-traitant ») et le Client agit en tant que responsable du traitement, fiduciaire commercial ou fiduciaire de données, tel que défini dans ces Lois Applicables sur la Protection des Données (« Responsable du Traitement ») en ce qui concerne ses propres données, ou (le cas échéant) les deux parties agissent en tant que Sous-traitants des données de leurs clients respectifs.

Les dispositions du présent DPA s'appliquent à toutes les activités de traitement des PII effectuées par Planview pour le compte du Client, en particulier aux fins de l'article 28 du Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (le « RGPD »), et conformément à toute autre loi sur la confidentialité et la protection des données à laquelle les parties peuvent être soumises en relation avec le traitement des PII dans le cadre des Services, y compris (si et dans la mesure applicable), mais sans s'y limiter : (i) la loi californienne sur la protection de la vie privée des consommateurs, Cal. Civ. Code §§ 1798.100 et suivants (la « CCPA »), telle que modifiée par la loi californienne sur les droits à la vie privée, Cal. Civ. Code §§ 1798.100 et suivants (la « CPRA ») et, collectivement, les « Lois Californiennes sur la Protection des Données » ; (ii) la loi indienne sur la protection des données personnelles numériques de 2023 (la « DPDPA ») ; (iii) la loi sur la protection des données, loi DIFC n° 5 de 2020, telle que modifiée (la « DPL ») ; (iv) la loi australienne sur la protection de la vie privée de 1988 (la « Loi sur la Protection de la Vie Privée ») ; (v) le règlement général sur la protection des données du Royaume-Uni tel que défini à l'article 3(10) de la loi sur la protection des données de 2018 (le « RGPD Britannique ») ; et (vi) la loi fédérale suisse sur la protection des données du 25 septembre 2020, telle que révisée (la « LPD Suisse ») (collectivement, les « Lois Applicables sur la Protection des Données »).

### 2. Comment s'Applique le Présent DPA

Le présent DPA est soumis aux conditions du SSA, auquel il est intégralement incorporé et dont il fait partie intégrante, et remplace toutes les conditions de traitement des données existantes dans le SSA ou dans tout addendum au SSA, ainsi que tous les accords, propositions ou déclarations antérieurs et contemporains, écrits ou oraux, concernant son objet, sauf indication contraire expresse dans les présentes. En cas de conflit entre le présent DPA et toute autre disposition du SSA concernant les PII, le présent DPA prévaudra.

### 3. Définitions

Tous les termes en majuscules utilisés dans les présentes ont la signification qui leur est donnée dans le SSA, dans le présent DPA ou dans l'une des Lois Applicables sur la Protection des Données, selon le cas.

### 4. Objet, Portée et Durée des Activités de Traitement

Les activités de traitement effectuées par Planview en tant que Sous-traitant dans le cadre du présent DPA concernent les Données du Client, y compris les PII, utilisées par le Client dans le cadre des Services pour la gestion de projets et de portefeuilles, le développement de produits digitaux, la planification des ressources et les opérations commerciales connexes. Ces activités de traitement comprennent (i) la collecte, le stockage et l'utilisation des PII pour l'identification des Utilisateurs ; (ii) la collecte, l'hébergement et le stockage des Données du Client et des informations liées aux projets, y compris les PII ; (iii) l'accès ou la consultation des Données du Client, y compris les PII, pour la fourniture de Services d'Assistance et/ou de Services Professionnels ; (iv) l'enregistrement, le stockage et l'examen des activités dans les systèmes d'information qui traitent ou accèdent aux Données du Client à des fins de sécurité et d'intégrité (comme décrit plus en détail à l'Annexe 3) ; et (v) la collecte et l'utilisation des Données du Client et des informations relatives au projet afin de fournir des fonctionnalités d'IA et de structure de données dans l'application et de garantir que les résultats répondent aux normes de cohérence et de qualité de Planview. Le traitement commence avec l'exécution du SSA et prend fin à la résiliation ou à l'expiration de la fourniture des Services, nonobstant la période supplémentaire de récupération des Données du Client décrite dans le SSA, pendant laquelle le DPA reste applicable. Planview peut conserver des copies de sauvegarde des Données du Client, y compris les PII, pendant une période limitée après la résiliation ou l'expiration du SSA, conformément à ses politiques de conservation des données, à condition que ces copies restent protégées par le présent DPA et ne soient pas consultées ou traitées à d'autres fins que le stockage de sauvegarde pour la reprise après sinistre.

Planview peut traiter les PII (obtenues directement auprès du Client ou indirectement auprès de tiers) à des fins d'administration, de facilitation et d'amélioration des Services de Planview, ce qu'elle fera en tant que Responsable du Traitement et ne sera donc pas soumise aux dispositions du présent DPA, afin de se conformer à ses propres obligations légales ou de poursuivre ses intérêts légitimes. Le Client doit mettre à la disposition de ses Utilisateurs finaux, employés, agents/sous-traitants autorisés, représentants et toute autre personne utilisant ou mentionnée dans les Services les informations nécessaires concernant le traitement de leurs PII par Planview en tant que Responsable du Traitement, en les renvoyant à la [Déclaration de Confidentialité](#) sur le site web de Planview. À titre d'information uniquement, le traitement par Planview des PII du Client à des fins d'administration, de facilitation et d'amélioration des Services comprend les catégories de données suivantes : (i) l'historique du Client, les données relatives à la facturation et aux paiements contractuels, les informations divulguées par des tiers (par exemple, des agences de référence en matière de crédit ou des annuaires publics), ainsi que les coordonnées et la signature des personnes de contact et des signataires autorisés du Client (le cas échéant), dans chaque cas si et dans la mesure où ces données contiennent des PII, à des fins de gestion interne de la relation client (CRM) de Planview ; et (ii) les données comportementales et les données de performance des Utilisateurs, qui sont agrégées et anonymisées afin de tirer des enseignements sur l'utilisation des Services dans le but de les améliorer.

### 5. Catégories de Données à Caractère Personnel

Les PII soumises aux activités de traitement de Planview comprennent généralement les catégories/types de données suivants : (i) coordonnées (par exemple, nom, adresse professionnelle, adresse e-mail professionnelle, numéro de téléphone professionnel, données de connexion et informations sur le fuseau horaire local) ; (ii) informations sur l'emploi (par exemple, nom de l'entreprise, intitulé du poste, grade/fonction, service, données démographiques et données de localisation) ; (iii) informations relatives aux projets et au portefeuille (par exemple, compétences, tarifs, temps et dépenses enregistrés, tâches et projets attribués, capacités et disponibilité des ressources) ; (iv) informations sur les systèmes informatiques et les appareils et données de trafic (qui peuvent inclure l'identifiant de l'Utilisateur, l'adresse IP et les informations de suivi des habitudes d'utilisation des logiciels, telles que les données dérivées des cookies) ; (v) le contenu des e-mails et les données de transmission des personnes concernées, qui sont disponibles de manière accessoire pour la fourniture des Services d'Assistance ; (vi) toute information personnelle fournie par l'Utilisateur aux Services.

Le Client, et non Planview, est seul responsable de déterminer quelles Données du Client, y compris les PII, le Client saisit ou traite via les Services. Planview n'assume aucune responsabilité pour le traitement de toute catégorie de PII autre que celles énumérées dans le paragraphe ci-dessus, y compris les catégories particulières de données à caractère personnel ou les PII sensibles telles que définies par les Lois Applicables sur la Protection des Données, dans la mesure où ces PII sont fournies ou traitées via les Services par le Client.

### 6. Catégories de Personnes Concernées

Les catégories de personnes concernées comprennent en général les employés du Client, les Utilisateurs (tels que définis dans le SSA), les consultants et autres agents autorisés, ou toute autre personne mentionnée dans les Services.

### 7. Mesures Techniques et Organisationnelles (« ToM »)

Les ToM garantissent un niveau de protection des données adapté au risque lié à la confidentialité, à la disponibilité et à l'intégrité des PII du Client, en fonction de la disponibilité et de la résilience des systèmes informatiques. L'état de l'industrie, les coûts de mise en œuvre, la nature, la portée et les finalités du traitement, ainsi que la probabilité de survenue et la gravité du risque pour les droits et libertés des personnes physiques déterminent les ToM appropriées à mettre en œuvre.

Les ToM de Planview, qui sont expressément approuvées par le Client, sont précisées dans l'Annexe 3 du présent DPA. Les mesures techniques sont soumises à des progrès techniques constants et à des développements ultérieurs. À cet égard, le Client autorise Planview à mettre en œuvre d'autres mesures techniques adéquates, à condition que cela ne réduise pas la sécurité des mesures définies. Planview surveillera périodiquement ses processus internes et ses mesures techniques afin de s'assurer que les activités de traitement sont menées conformément aux exigences des lois applicables en matière de protection de la vie privée pour la protection des droits des personnes concernées.

### 8. Principes des Activités de Traitement et Droits des Personnes Concernées

Les activités de traitement doivent être effectuées selon les instructions du Client. Par conséquent, Planview ne peut effectuer, conserver, rectifier, effacer ou limiter le traitement des PII que sur instruction écrite du Client, comme décrit dans le présent DPA, et/ou conformément au SSA, sauf si la loi applicable à laquelle Planview est soumise l'y oblige. Dans ce cas, Planview informera le Client de cette obligation légale avant le traitement, sauf si cette loi lui interdit d'en informer le Client pour des raisons importantes d'intérêt public. Planview informera immédiatement le Client si, à son avis, une instruction enfreint une loi applicable, y compris le RGPD et/ou d'autres Lois Applicables sur la Protection des Données.

## Accord sur la confidentialité, la sécurité et le traitement des données (« DPA »)

Dans la mesure où une personne concernée contacte directement Planview pour exercer ses droits en vertu des Lois Applicables sur la Protection des Données, Planview demandera immédiatement à la personne concernée de soumettre sa demande au Client. Nonobstant ce qui précède, Planview aidera le Client à remplir son obligation de répondre aux demandes des personnes concernées souhaitant exercer leurs droits, dans la mesure du possible, en tenant compte de la nature du traitement et des PII effectivement consultées et traitées par Planview, et à condition que le Client demande expressément cette assistance par le biais d'instructions claires et documentées transmises à Planview en temps utile.

### 9. Protection des Données en Californie

Dans la mesure où Planview traite des PII du Client relatif à des personnes résidant en Californie, Planview se conformera aux dispositions applicables des Lois Californiennes sur la Protection des Données. Aux fins des Lois Californiennes sur la Protection des Données, les parties conviennent que (i) Planview est un « prestataire de services » dans l'exécution de ses obligations, et non un « tiers » ou un « sous-traitant », (ii) le Client est une « entreprise », et (iii) le transfert des PII du Client à Planview ne doit pas être considéré comme une « vente » ou un « partage ».

Dans la mesure requise par les Lois Californiennes sur la Protection des Données, Planview (a) fournira le même niveau de protection de la confidentialité que celui requis par les Lois Californiennes sur la Protection des Données ; (b) accordera au Client le droit de prendre des mesures raisonnables et appropriées pour s'assurer que Planview utilise les PII du Client d'une manière conforme aux obligations du Client en vertu des Lois Californiennes sur la Protection des Données ; (c) informera le Client si Planview détermine qu'elle ne peut plus respecter ses obligations en vertu des Lois Californiennes sur la Protection des Données ; et (d) accordera au Client le droit, moyennant un préavis raisonnable, de prendre des mesures raisonnables et appropriées pour mettre fin à toute utilisation non autorisée des PII du Client et y remédier.

En tant que prestataire de services, Planview s'engage à ne pas (w) vendre ou partager les PII du Client ; (x) conserver, utiliser ou divulguer les PII du Client à des fins autres que les « fins commerciales », y compris conserver, utiliser ou divulguer les PII du Client à des fins commerciales autres que les fins commerciales ou autrement autorisées par la CPRA ; (y) conserver, utiliser ou divulguer les PII du Client en dehors de la relation commerciale directe entre Planview et le Client ; ou (z) combiner les PII du Client que Planview reçoit du Client ou en son nom avec les PII qu'elle reçoit d'une ou de plusieurs autres personnes ou en leur nom, ou qu'elle recueille à partir de ses propres interactions avec le consommateur, étant entendu que Planview peut combiner les PII pour atteindre tout objectif commercial tel que défini dans les règlements adoptés conformément au paragraphe (10) de la sous-section (a) du Cal. Civ. Code § 1798.185, sauf dans les cas prévus au paragraphe (6) de la subdivision (e) du Cal. Civ. Code § 1798.140 et dans les réglementations adoptées par l'Agence californienne de protection de la vie privée.

### 10. Autres Lois Américaines sur la Protection des Données

Dans la mesure où Planview traite des PII relatives à des personnes physiques qui sont des « consommateurs » au sens de la loi sur la protection de la vie privée du Colorado (Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 et suivants), la loi sur la protection des données du Connecticut, loi publique n° 22-15, la loi sur la protection des consommateurs de l'Utah, Utah Code Ann. §§ 13-61-101 et suivants, et la loi sur la protection des données des consommateurs de Virginie, Va. Code Ann. §§59.1-575 et suivants (collectivement, les « Lois sur la Protection des Données des Consommateurs »), respectivement, et à la date d'entrée en vigueur respective de la loi applicable sur la Protection des Données des Consommateurs, Planview se conformera aux exigences des Lois sur la Protection des Données des Consommateurs.

### 11. Sous-traitants Secondaires

Planview peut faire appel à des sociétés affiliées à Planview et/ou à des prestataires de services tiers (collectivement, les « Sous-traitants Secondaires »), dispersés dans le monde entier, pour effectuer des activités de traitement spécifiques pour le compte du Client et en relation avec les Services.

Le Client accorde à Planview une autorisation générale pour engager des Sous-traitants Secondaires afin d'exécuter des tâches spécifiques en rapport avec les Services, sous réserve des conditions suivantes : (i) un accord contractuel doit être conclu entre Planview et le Sous-traitant Secondaire, en vertu duquel ce dernier est soumis aux mêmes exigences en matière de protection des données que Planview en ce qui concerne les PII en vertu du présent DPA et de toute législation applicable ; et (ii) Planview peut ajouter et/ou remplacer des Sous-traitants Secondaires existants par de nouveaux Sous-traitants Secondaires fournissant des services et des garanties équivalents en termes de ToM mises en œuvre pour protéger les PII, lorsque (a) Planview informe le Client de ce changement par un préavis approprié en l'annonçant au moins trente (30) jours à l'avance sur le [site web Planview Status](#), auquel le Client s'engage par la présente à s'abonner pour recevoir les mises à jour ; et (b) le changement n'est pas effectué uniquement pour la commodité de Planview, mais pour la nécessité d'améliorer ou de fournir les Services sans modification.

Le Client peut raisonnablement s'opposer au remplacement ou à l'ajout de Sous-traitants Secondaires pour des raisons liées à la conformité du Client ou de Planview aux Lois Applicables sur la Protection des Données, en envoyant une notification écrite de cette opposition à [privacy@planview.com](mailto:privacy@planview.com) dans les trente (30) jours suivant la réception de la notification du changement. Dès réception d'une objection valide, les parties travailleront ensemble de bonne foi pour trouver une solution commercialement raisonnable, telle que la fourniture des Services sans recourir au Sous-traitant Secondaire faisant l'objet de l'objection. Si aucune solution de ce type n'est envisageable, le Client peut alors résilier, sans pénalité, le(s) Bon(s) de Commande et/ou le(s) Cahier(s) des Charges applicables uniquement en ce qui concerne les Services qui ne peuvent être fournis sans recourir au Sous-traitant Secondaire faisant l'objet de l'objection.

Aux fins de l'autorisation préalable générale accordée ci-dessus, les Sous-traitants Secondaires autorisés de Planview à un moment donné sont répertoriés sur [le site web Trust de Planview](#). Planview est entièrement responsable envers le Client de l'exécution des activités de traitement des Sous-traitants Secondaires liées aux Données du Client, y compris les PII.

### 12. Obligations de Planview

**12.1 Confidentialité.** Planview ne confie le traitement des PII du Client qu'à des employés et sous-traitants qui ont été liés par des obligations de confidentialité et qui ont préalablement pris connaissance des dispositions relatives à la confidentialité et à la protection des données applicables à leur travail.

**12.2 Assistance et Informations.** Sur demande écrite claire du Client envoyée par e-mail à [privacy@planview.com](mailto:privacy@planview.com), et en tenant compte de la nature du traitement et des informations à sa disposition, Planview coopérera avec le Client et l'aidera à démontrer et à garantir le respect de ses obligations en matière de confidentialité et de protection des données. En particulier, Planview aidera le Client à (i) respecter l'obligation d'assurer la sécurité du traitement, en maintenant et en mettant à jour (si nécessaire) ses propres ToM afin de garantir un niveau de protection des données adapté au risque lié aux PII du Client ; (ii) remplir l'obligation du Client de notifier les violations de données aux autorités de contrôle et aux personnes concernées, comme détaillé à la Section 15 du présent DPA ; et (iii) réaliser des analyses d'impact relatives à la protection des données (AIPD) et consulter l'autorité de contrôle, lorsque la loi l'exige, en fournissant des informations adéquates sur le traitement des PII en rapport avec les Services.

**12.3 Divulgué aux Autorités Gouvernementales.** Planview informera le Client de toute demande de divulgation des PII du Client émanant d'un organisme gouvernemental ou réglementaire ou d'une autorité chargée de l'application de la loi (y compris toute autorité de contrôle de la protection des données), sauf si la loi ou une ordonnance juridiquement contraignante de cet organisme ou de cette agence l'interdit. Si la loi interdit à Planview de fournir une telle notification, Planview déploiera des efforts commercialement raisonnables pour obtenir une dérogation à cette interdiction afin de permettre cette communication. Si Planview estime que la demande de divulgation n'est pas juridiquement contraignante, Planview ne divulguera aucune donnée du Client, sauf instruction contraire de ce dernier.

Dans tous les cas, si le Client souhaite que Planview informe directement toute personne concernée (i) de toute demande de divulgation des PII du Client par un organisme gouvernemental ou réglementaire ou une autorité chargée de l'application de la loi, ou (ii) de tout accès direct aux PII du Client par les autorités publiques, le Client doit alors en informer Planview de manière expresse et claire par écrit en envoyant un e-mail à [privacy@planview.com](mailto:privacy@planview.com).

### 13. Scénarios de Transfert de Données et Mécanismes de Transfert Applicables

Le Client est conscient et comprend que la nature mondiale des Services peut nécessiter des transferts internationaux des PII du Client, et les parties conviennent d'adopter les mesures appropriées pour garantir la conformité avec les exigences en matière de transfert international de données en vertu des Lois Applicables sur la Protection des Données. La présente Section 13 régit les scénarios de transfert de données pertinents et les mécanismes de transfert adoptés dans chacun d'entre eux. Dans la mesure où l'organisation des Services fournis par Planview au Client n'entraîne aucun des scénarios décrits dans la présente Section, les mécanismes de transfert et la Section correspondante ne s'appliquent pas.

**13.1 Transferts de Données Soumis à des Décisions d'Adéquation.** Le Client peut librement transférer des PII soumises au RGPD, au RGPD Britannique, à la LPD Suisse et/ou à la DPL à Planview ou à l'une de ses filiales situées dans un pays tiers qui a été déterminé par la Commission européenne, le secrétaire d'État britannique, le Conseil fédéral suisse et/ou le commissaire à la protection des données du DIFC, selon le cas, comme offrant un niveau adéquat de protection des données, y compris, mais sans s'y limiter, les États-Unis d'Amérique dans le cadre de la protection des données UE-États-Unis (DPF), de l'extension britannique au DPF UE-États-Unis et du DPF Suisse-États-Unis, ou tout cadre, certification, décision d'adéquation ou autre mécanisme de transfert légal qui pourrait être adopté à l'avenir pour remplacer ou compléter le DPF.

**13.2 Transferts de Données Soumis au RGPD.** Lorsque le Client transfère des PII soumises au RGPD à Planview ou à l'une de ses filiales situées dans un pays qui ne garantit pas un niveau adéquat de protection des données en vertu du RGPD, les parties doivent adopter les clauses contractuelles types énoncées dans la Décision d'Exécution (UE) 2021/914 de la Commission Européenne du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers (ci-après dénommées « Clauses Contractuelles Types de l'UE ») comme mécanisme de transfert. Lorsqu'elles sont adoptées entre les parties, les Clauses Contractuelles Types de l'UE doivent suivre le modèle deux (Responsable du Traitement à Sous-traitant) ou (le cas échéant) le modèle trois (Sous-traitant à Sous-traitant) dans les conditions établies dans la présente Annexe 1, clause 1.

## Accord sur la confidentialité, la sécurité et le traitement des données (« DPA »)

**13.3 Transferts de Données Soumis à la LPD Suisse.** Lorsque le Client transfère des PII soumises à la LPD Suisse à Planview ou à l'une de ses filiales situées dans un pays qui ne garantit pas un niveau adéquat de protection des données en vertu de la Loi Applicable sur la Protection des Données, les parties doivent adopter les Clauses Contractuelles Types de l'UE telles qu'établies à l'Annexe 1, clause 2, comme mécanisme de transfert.

**13.4 Transferts de Données Soumis au RGPD Britannique.** Lorsque le Client transfère des PII soumises au RGPD Britannique à Planview ou à l'une de ses filiales situées dans un pays qui ne garantit pas un niveau adéquat de protection des données en vertu de la Loi Applicable sur la Protection des Données, les parties doivent adopter les Clauses Contractuelles Types de l'UE, complétées par l'addendum sur les transferts internationaux de données aux clauses contractuelles types de la Commission européenne, publié par le commissaire à l'information en vertu de l'article 119A(1) de la loi britannique de 2018 sur la protection des données, telle que mise à jour, modifiée, remplacée ou abrogée de temps à autre par le gouvernement britannique (l'« IDTA Britannique »), comme établi à l'Annexe 1, clause 3, en tant que mécanisme de transfert.

**13.5 Transferts de Données Soumis à la DIFC DPL.** Lorsque le Client transfère des PII soumises à la DPL à Planview ou à l'une de ses filiales situées dans un pays qui ne garantit pas un niveau adéquat de protection des données en vertu de la Loi Applicable sur la Protection des Données, les parties adopteront les Clauses Contractuelles Types de l'UE, complétées par l'IDTA Britannique le cas échéant, telles qu'établies à l'Annexe 1, clause 4, comme mécanisme de transfert.

**13.6 Transferts Ultérieurs de Données à Des Sous-traitants Secondaires.** Lorsque, aux fins de la Section 11 du présent DPA, Planview transfère les PII du Client à un Sous-traitant Secondaire situé dans un pays qui ne garantit pas un niveau adéquat de protection des données en vertu de la Loi Applicable sur la Protection des Données, Planview conclura les Clauses Contractuelles Types de l'UE du module trois (Sous-traitant à Sous-traitant), complétées par l'IDTA Britannique et/ou avec les adaptations nécessaires conformément à la FADP Suisse ou à la DPL, selon le cas, avec les Sous-traitants Secondaires qui accèdent ou traitent de toute autre manière les PII du Client en dehors de l'EEE, du Royaume-Uni, de la Suisse et/ou du DIFC, selon le cas. Nonobstant ce qui précède, Planview et le Sous-traitant Secondaire peuvent également mettre en œuvre tout autre mécanisme de transfert de données valide reconnu par les Lois Applicables sur la Protection des Données, à condition que ce mécanisme garantisse un niveau de protection des PII du Client au moins équivalent à celui offert par les Clauses Contractuelles Types de l'UE.

### 14. Contact en Matière de Protection des Données

Planview a désigné un délégué à la protection des données (DPO) chargé de veiller au respect des Lois Applicables sur la Protection des Données et de répondre aux questions concernant le traitement des PII par Planview. Le DPO de Planview peut être contacté à l'adresse [privacy@planview.com](mailto:privacy@planview.com).

### 15. Violations de Données

Planview informera le Client sans délai après avoir pris connaissance d'une violation de données susceptible de compromettre la confidentialité, la disponibilité et/ou l'intégrité des Données du Client et/ou la protection des PII. Planview collaborera avec le Client et répondra à toutes les demandes raisonnables d'informations ou de mises à jour formulées par le Client, dans la mesure où cela n'interfère pas avec le travail de Planview consistant à enquêter sur la violation et à en limiter les effets. Planview répondra aux questions du Client sans délai injustifié, dans la mesure du possible et aussi souvent que raisonnablement nécessaire, jusqu'à ce que la violation ait été corrigée.

### 16. Pouvoirs de Contrôle du Client

Planview s'engage à fournir au Client les informations légalement requises concernant le traitement des PII afin de démontrer le respect par Planview de ses obligations en matière de protection des données et, en particulier, de démontrer l'exécution des ToM, sur demande écrite du Client. La preuve de ces mesures, qui concernent non seulement les PII du Client, mais aussi, plus généralement, les Données du Client, peut être fournie par une certification ou un rapport approprié délivré par un organisme tiers indépendant d'audit de la sécurité informatique ou de la protection des données. Le Client utilisera les certificats et/ou rapports d'évaluation externe de Planview (ISO 27001, 27701 et/ou SOC2 Type 2) à des fins d'audit, d'inspection et de questionnaire. Si des questions subsistent ou si des éclaircissements supplémentaires sont nécessaires, les parties détermineront une procédure mutuellement acceptable pour l'examen de tout point en suspens, tel que des inspections supplémentaires, qui pourront être effectuées par un auditeur externe (à condition que cet auditeur soit lié par un accord de confidentialité), qui sera désigné dans chaque cas individuel moyennant un préavis écrit de trente (30) jours à Planview (sauf si un délai plus court est requis pour satisfaire à une exigence légale ou à une demande d'une autorité de contrôle ou d'une autorité gouvernementale), et sera mené de manière à perturber le moins possible la fourniture des Services par Planview et ses autres activités commerciales normales.

Si le Client demande à Planview de répondre à des questionnaires ou à des évaluations en matière de confidentialité et de sécurité qui ne peuvent être facilement remplis en se référant aux politiques et procédures existantes de Planview ou aux résultats d'évaluation sommaires mentionnés dans les présentes, Planview aura alors le droit de facturer au Client le temps consacré par son personnel à cette tâche.

### 17. Résiliation

À la fin des activités de traitement, Planview résiliera le compte des Services par Abonnement du Client dans le(s) Produit(s) Planview et supprimera tout accès au système par le Client et les Utilisateurs. Le cas échéant, au choix du Client, Planview restituera ou détruira toutes les Données du Client liées aux Services qui sont en sa possession, y compris les PII, d'une manière conforme à la protection des données. Il en va de même pour tous les éléments connexes liés aux tests, aux déchets, aux éléments redondants et aux éléments mis au rebut. Toutes les Données du Client sont supprimées dès que possible après la résiliation ou l'expiration du contrat, nonobstant la conservation par Planview de copies de sauvegarde des Données du Client pendant une période limitée conformément à la Section 4 du présent DPA, et à moins qu'une loi applicable à laquelle Planview soit soumise n'exige le stockage de ces données (y compris les PII). Une assurance écrite de la suppression ou de la destruction de toutes les Données du Client sera fournie si le Client en fait la demande écrite au DPO de Planview.

### 18. Divers

Le présent DPA est régi par la loi qui régit le SSA et tout litige entre les parties sera traité conformément aux dispositions du SSA.

Le Client peut résilier le présent DPA et/ou le SSA dans les cas suivants : (i) Planview enfreint de manière substantielle l'une des déclarations ou garanties qu'il a données en vertu du présent DPA et ne remédie pas à cette violation dans les quatre-vingt-dix (90) jours suivant la réception de la notification du Client ; ou (ii) une autorité de contrôle ou autre autorité réglementaire ou autre tribunal ou cour constate qu'il y a eu violation des lois applicables dans cette juridiction en raison du traitement des PII par Planview ou le Client.

## ANNEXE 1

### Clauses Contractuelles Types

#### 1. Clauses Contractuelles Types de l'UE

Aux fins de la Section 13.2 du présent DPA, les parties conviennent que les Clauses Contractuelles Types de l'UE, module deux (Responsable du Traitement à Sous-traitant) et module trois (Sous-traitant à Sous-traitant) sont incorporées aux présentes par référence. Le Client est l'exportateur de données et Planview est l'importateur de données, et les parties conviennent de ce qui suit :

##### 1.1 Clause d'Ancre

L'option prévue à la clause 7 des Clauses Contractuelles Types de l'UE ne s'applique pas.

##### 1.2 Documentation et Conformité

Les parties conviennent que les exigences en matière de documentation et de conformité décrites à la clause 8.9 des Clauses Contractuelles Types de l'UE seront mises en œuvre conformément à la Section 16 du présent DPA.

##### 1.3 Autorisation Générale d'Utilisation de Sous-traitants Secondaires

Aux fins de la clause 9 des Clauses Contractuelles Types de l'UE, l'option 2 s'applique. Aux fins de la clause 9 (a) des Clauses Contractuelles Types de l'UE, Planview dispose d'une autorisation générale pour engager des Sous-traitants Secondaires conformément à la Section 11 du présent DPA. Planview répertorie les Sous-traitants Secondaires sur [son site web Trust](#) et toute modification ou ajout prévu à la liste sera communiqué au Client au moins trente (30) jours à l'avance. Lorsque le module 3 (Sous-traitant à Sous-traitant) des Clauses Contractuelles Types de l'UE s'applique entre le Client et Planview, conformément au premier paragraphe de la Section 1 du présent DPA, le Client garantit par la présente qu'il a obtenu l'autorisation générale du Responsable du Traitement pour que Planview engage des Sous-traitants Secondaires conformément à la Section 11 du présent DPA, et s'engage en outre à informer spécifiquement le Responsable du Traitement par écrit de toute modification ou tout ajout à la liste des Sous-traitants Secondaires autorisés de Planview dont le Client est informé, au plus tard dans les vingt (20) jours suivant la réception de la notification de Planview, comme décrit à la clause 1.4 de la présente Annexe.

Lorsque Planview conclut des Clauses Contractuelles Types de l'UE, module 3 (Sous-traitant à Sous-traitant) avec ses Sous-traitants Secondaires, le Client accorde à Planview le pouvoir de fournir une autorisation générale en son nom pour le recours à des sous-traitants par des Sous-traitants Secondaires précédemment engagés dans la fourniture des Services, ainsi que le pouvoir d'approuver l'ajout ou le remplacement de l'un de ces sous-traitants.

##### 1.4 Notification Relative aux Nouveaux Sous-traitants Secondaires et Droit d'Opposition

Aux fins de la clause 9(a) des Clauses Contractuelles Types de l'UE, le Client accepte que les notifications relatives aux ajouts ou modifications apportés aux Sous-traitants Secondaires de Planview soient publiées sur le [site Web Planview Status](#), auquel le Client s'engage à s'abonner pour recevoir les mises à jour, conformément à la Section 11 du présent DPA. Les deux parties conviennent que les objections au remplacement ou à l'ajout de Sous-traitants Secondaires sont également régies par la Section 11 du présent DPA.

##### 1.5 Recours

L'option prévue à la clause 11 des Clauses Contractuelles Types de l'UE ne s'applique pas.

##### 1.6 Supervision

Aux fins de la clause 13 des Clauses Contractuelles Types de l'UE, lorsque le Client n'est pas établi dans un État membre de l'UE, mais relève du champ d'application territorial du RGPD conformément à son article 3, paragraphe 2, sans toutefois être tenu de désigner un représentant conformément à l'article 27, paragraphe 2, du RGPD, et dans le cas où au moins une des personnes concernées dont les données à caractère personnel sont transférées en vertu du présent DPA se trouve en Suède, l'autorité suédoise chargée de la protection de la vie privée (IMY) est l'autorité indiquée à l'annexe I.C.

##### 1.7 Loi Applicable

Aux fins de la clause 17 des Clauses Contractuelles Types de l'UE, l'option 1 s'applique et la loi applicable est la loi suédoise.

##### 1.8 Choix du For et de la Juridiction

Les parties conviennent que, aux fins de la clause 18 des Clauses Contractuelles Types de l'UE, les tribunaux compétents sont les tribunaux suédois.

##### 1.9 Description du Transfert et Mesures Techniques et Organisationnelles

Les informations décrites aux Annexes 2 et 3 du présent DPA sont intégrées respectivement aux annexes I et II des Clauses Contractuelles Types de l'UE.

#### 2 Droit Suisse

Aux fins de la Section 13.3 du présent DPA, les parties conviennent que les Clauses Contractuelles Types de l'UE, module deux (Responsable du Traitement à Sous-traitant) et module trois (Sous-traitant à Sous-traitant) s'appliquent selon les termes établis à la clause 1 de la présente Annexe 1, avec les adaptations nécessaires décrites dans les clauses suivantes. Le Client est l'exportateur de données et Planview l'importateur de données, et les parties conviennent des adaptations suivantes :

##### 2.1 Supervision

Aux fins de la clause 13 des Clauses Contractuelles Types de l'UE et dans la mesure où le transfert de données est régi par la LPD Suisse, le Préposé fédéral à la protection des données et à la transparence est l'autorité indiquée à l'annexe I.C.

##### 2.2 Loi Applicable aux Réclamations Contractuelles

Aux fins de la clause 17 des Clauses Contractuelles Types de l'UE, le droit suédois s'applique.

##### 2.3 Lieu de Juridiction Pour les Actions Entre les Parties

Conformément à la clause 18 (b) des Clauses Contractuelles Types de l'UE, la Suède est le lieu de juridiction pour les actions entre les parties.

##### 2.4 Lieu de Juridiction Pour les Actions Intentées par les Personnes Concernées

Le terme « État membre » ne doit pas être interprété de manière à exclure les personnes concernées en Suisse de la possibilité d'intenter une action en justice pour faire valoir leurs droits dans leur lieu de résidence habituel, conformément à la clause 18 (c) des Clauses Contractuelles Types de l'UE.

#### 3 Loi Britannique

Aux fins de la Section 13.4 du présent DPA, les parties conviennent que les Clauses Contractuelles Types de l'UE, telles que complétées par l'IDTA Britannique, sont incorporées aux présentes par référence. Le Client est l'exportateur de données et Planview l'importateur de données, et les parties conviennent des adaptations suivantes :

##### Partie 1 Tableau 1

- (i) La date de début est la date indiquée sur le Bon de Commande et/ou le Cahier des Charges applicable.
- (ii) L'exportateur est le Client, tel que défini à la Section 1 de l'Annexe 2. L'importateur est Planview, tel que défini à la Section 1 de l'Annexe 2.
- (iii) Le contact principal de l'exportateur est celui défini à la Section 1 de l'Annexe 2.
- (iv) La personne-ressource principale de l'importateur est Cajs Weibring, Avocate Générale Adjointe EMEA, APAC et DPO, [privacy@planview.com](mailto:privacy@planview.com).
- (v) Les signatures sont celles indiquées dans le SSA.

##### 3.2 Tableau 2

Les parties choisissent les Clauses Contractuelles Types de l'UE, y compris les informations en annexe, et seuls les modules, clauses ou dispositions facultatives suivants des Clauses Contractuelles Types de l'UE sont mis en œuvre aux fins du présent IDTA :

- (i) Modules en vigueur – Deux et trois.
- (ii) Clause 7 – Voir Section 1.1 ci-dessus.
- (iii) Clause 9 – Voir Section 1.3 ci-dessus.
- (iv) Clause 11 – Voir Section 1.5 ci-dessus.

##### 3.3 Tableau 3

- (i) Annexe 1A : Voir Annexe 2.

## Accord sur la confidentialité, la sécurité et le traitement des données (« DPA »)

- (ii) Annexe 1B : Voir Annexe 2.
- (iii) Annexe II : Voir Annexe 3.
- (iv) Annexe III : Sans objet.

### 3.4 Tableau 4

L'importateur et l'exportateur peuvent mettre fin au présent accord IDTA.

### Partie 2

Clauses obligatoires de l'addendum approuvé, à savoir le modèle d'addendum B.1.0 publié par l'ICO et présenté au Parlement conformément à l'article 119A de la loi de 2018 sur la protection des données le 2 février 2022, tel que révisé en vertu de l'article 18 de ces clauses obligatoires.

### 4 Loi DIFC

Comme indiqué à la Section 13.5 du présent DPA concernant les transferts de données à caractère personnel vers un pays tiers qui n'est pas encore considéré comme adéquat par le commissaire à la protection des données du DIFC, les clauses contractuelles types (CCT) disponibles via le lien ci-dessous sont réputées annexées au présent DPA et contraignantes pour les parties afin de se conformer à l'article 27 de la LPD. Le Client est l'exportateur de données et Planview l'importateur de données, et les parties conviennent des adaptations suivantes :

#### 4.1 Clauses Contractuelles Types Applicables

- ☐ [CCT du DIFC](#)
- ☒ [Clauses Contractuelles Types de l'UE](#) – Modules sélectionnés comme convenu par les parties dans la section 1 ci-dessus.
- ☒ [CCT britanniques](#) / IDTA Britannique – Sélections appropriées et/ou IDTA Britannique complétée comme indiqué dans la section 3 ci-dessus.
- ☐ Autres clauses contractuelles types (à fournir par l'exportateur ou l'importateur).

#### 4.2 Représentants des Parties

- (i) Le représentant de l'exportateur de données est celui désigné à la Section 1 de l'Annexe 2. Aucune autre information n'est nécessaire pour que le contrat soit contraignant et la signature est celle prévue dans le SSA.
- (ii) Le représentant de l'importateur de données est Cajsia Weibring, Avocate Générale Adjointe EMEA, APAC et DPO, [privacy@planview.com](mailto:privacy@planview.com). Aucune autre information n'est nécessaire pour que le contrat soit contraignant et la signature est celle établie dans le SSA.

#### 4.3 Annexes

- (i) Annexe 1 – Voir Annexe 2.
- (ii) Annexe 2 – Voir Annexe 3.
- (iii) Annexe 3 – Sans objet.

### 5 Conflit

Les Clauses Contractuelles Types de l'UE doivent être appliquées conformément au présent DPA, sauf indication contraire. En cas de conflit ou d'incohérence entre le corps du présent DPA et les Clauses Contractuelles Types de l'UE, ces dernières prévaudront.

**ANNEXE 2**

**Description du Transfert**

**1. Liste des Parties**

**Exportateur(s) de données :**

Nom : Client, tel qu'établi dans le SSA

Adresse : Tel que défini dans le SSA

Nom, fonction et coordonnées de la personne à contacter : les coordonnées associées au compte Planview du Client ou telles que spécifiées dans le SSA

Activités pertinentes pour les données transférées en vertu des présentes clauses : Contrat de Services tel que défini plus en détail dans le SSA

Signature et date : comme indiqué dans le SSA

Rôle (responsable du traitement/sous-traitant) : Responsable du Traitement (Module deux) et/ou Sous-traitant (Module trois)

**Importateur(s) de données :**

Nom : Entité Planview établie dans le SSA

Adresse : Tel que défini dans le SSA

Nom, fonction et coordonnées de la personne à contacter : Cajsja Weibring, Avocate Générale Adjointe EMEA, APAC et DPO, [privacy@planview.com](mailto:privacy@planview.com)

Activités liées aux données transférées en vertu des présentes clauses : Exécution des Services

Signature et date : comme indiqué dans le SSA

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

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

Employés du Client, Utilisateurs (tels que définis dans le SSA), consultants autorisés et autres agents, ou autres personnes mentionnées dans les Services, comme décrit plus en détail dans le SSA et dans le présent DPA.

**3. Catégories de données à caractère personnel transférées :**

(i) coordonnées (par exemple, nom, adresse professionnelle, adresse e-mail professionnelle, numéro de téléphone professionnel, données de connexion et informations sur le fuseau horaire local) ; (ii) informations sur l'emploi (par exemple, nom de l'entreprise, intitulé du poste, grade/fonction, service, données démographiques et données de localisation) ; (iii) informations relatives aux projets et au portefeuille (par exemple, compétences, tarifs, temps et dépenses enregistrés, tâches et projets attribués, capacités et disponibilité des ressources) ; (iv) informations sur les systèmes informatiques et les appareils et données de trafic (qui peuvent inclure l'identifiant de l'utilisateur, l'adresse IP et les informations de suivi des habitudes d'utilisation des logiciels, telles que les données dérivées des *cookies*) ; (v) le contenu des e-mails et les données de transmission de la personne concernée, qui sont disponibles de manière accessoire pour la fourniture de Services d'Assistance et/ou de Services Professionnels ; (vi) toute information personnelle fournie par les Utilisateurs aux Services.

**4. Données sensibles transférées (le cas échéant) et restrictions ou mesures de protection appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, telles que, par exemple, une limitation stricte de la finalité, des restrictions d'accès (y compris l'accès réservé au personnel ayant suivi une formation spécialisée), la conservation d'un registre des accès aux données, des restrictions pour les transferts ultérieurs ou des mesures de sécurité supplémentaires :**  
Sans objet

**5. La fréquence du transfert (par exemple, si les données sont transférées de manière ponctuelle ou continue) :**

De manière continue lorsque les Services sont utilisés.

**6. Nature du traitement :**

(i) collecte, stockage et utilisation des PII pour l'identification des Utilisateurs ; (ii) collecte, hébergement et stockage des Données du Client et des informations relatives aux projets, y compris les PII ; (iii) accès ou consultation des Données du Client, y compris les PII, pour la fourniture de Services d'Assistance et/ou de Services Professionnels ; (iv) enregistrement, stockage et examen des activités dans les systèmes d'information qui traitent ou accèdent aux Données du Client à des fins de sécurité et d'intégrité (comme décrit plus en détail à l'Annexe 3) ; et (v) collecte et utilisation des Données du Client et des informations relatives au projet afin de fournir des fonctionnalités d'IA et de structure de données dans l'application et de garantir que les résultats répondent aux normes de cohérence et de qualité de Planview.

**7. Finalité(s) du transfert et du traitement ultérieur des données :**

Exécuter et respecter les engagements du SSA envers le Client.

**8. Période pendant laquelle les données à caractère personnel seront conservées ou, si cela n'est pas possible, critères utilisés pour déterminer cette période :**

Pendant toute la durée de la fourniture des Services, plus la période supplémentaire de récupération des Données du Client telle que décrite dans le SSA. Planview peut conserver des copies de sauvegarde des Données du Client, y compris les PII, pendant une période limitée après la résiliation ou l'expiration de la fourniture des Services, conformément à ses politiques de conservation des données, à condition que ces copies restent protégées par le présent DPA et ne soient pas consultées ou traitées à d'autres fins que le stockage de sauvegarde pour la reprise après sinistre.

**9. Pour les transferts vers des sous-traitants ou des sous-traitants ultérieurs, précisez également l'objet, la nature et la durée du traitement :**

Pour exécuter et remplir les engagements du SSA, pendant toute la durée de la fourniture des Services. Des informations détaillées sur les différentes activités de traitement soumises aux transferts, y compris leur objet et leur nature, sont précisées sur [le site web Trust de Planview](#) consacré aux sous-traitants.



## ANNEXE 3

### Mesures techniques et organisationnelles

#### Mesures techniques et organisationnelles, y compris les mesures techniques et organisationnelles visant à garantir la sécurité des données.

Description des mesures techniques et organisationnelles mises en œuvre par le ou les importateurs de données (y compris toute certification pertinente) pour garantir un niveau de sécurité approprié, 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 physiques.

Planview mettra en place des mesures de protection administratives, physiques et techniques afin de garantir la sécurité, la confidentialité, la disponibilité et l'intégrité des Données du Client, y compris les PII (collectivement, les « **Mesures de Sécurité** »).

#### 1. Gestion de la Sécurité

Planview maintiendra un programme de gestion de la sécurité efficace soumis à l'examen, au soutien et à la responsabilité de la direction en ce qui concerne les politiques et pratiques connexes, comprenant :

- (i) Une politique écrite en matière de sécurité de l'information qui respecte les lois et réglementations applicables, satisfait ou dépasse les normes industrielles applicables et qui, au minimum, inclut des rôles et responsabilités définis en matière de sécurité de l'information ainsi qu'un programme formel et efficace de gestion des risques ;
- (ii) La réalisation d'évaluations des risques de tous les systèmes traitant les Données du Client ;
- (iii) La réalisation d'audits internes pour mesurer l'efficacité des contrôles ;
- (iv) L'examen des incidents de sécurité, y compris la détermination efficace de la cause profonde et des mesures correctives ;
- (v) Un cadre de contrôle formel basé sur une norme externe, telle que SOC 2, ISO 27001 ou d'autres cadres pertinents ; et
- (vi) Un processus permettant de documenter la non-conformité aux Mesures de Sécurité et d'identifier et de quantifier les risques et les plans d'atténuation. Le plan d'atténuation doit être approuvé par le directeur des systèmes d'information (DSI) de Planview, le responsable de la sécurité des systèmes d'information (RSSI) de Planview ou un employé autorisé de Planview qui peut accepter la responsabilité et l'obligation de rendre compte au nom de Planview.

#### 2. Installations

Planview veillera à ce que les installations de ses fournisseurs de services de centres de données tiers qui stockent ou traitent les Données du Client disposent de mesures suffisantes pour :

- (i) Se protéger contre tout accès physique non autorisé, tout dommage et toute interférence à l'aide de contrôles de sécurité physiques pouvant inclure, sans s'y limiter, un accès par carte magnétique, une alimentation électrique redondante, une infrastructure redondante et des murs extérieurs solides ;
- (ii) limiter et contrôler toutes les entrées et sorties à l'aide de mesures pouvant inclure, sans s'y limiter, des agents de sécurité sur place, des lecteurs de badges, des serrures électroniques et un système de vidéosurveillance (CCTV) ; et
- (iii) Garantir que les systèmes traitant les Données du Client sont physiquement isolés des zones de service qui fournissent des points d'accès à l'intérieur et à l'extérieur des locaux.

#### 3. Accès, Contrôle et Surveillance des Employés

Planview fournira des méthodes d'authentification et des pratiques qui comprennent, au minimum, les contrôles et les mesures de protection suivants appliqués aux employés et aux sous-traitants de Planview (collectivement, les « représentants de Planview ») :

- (i) Conformément à la loi applicable et sous réserve de la politique de Planview en matière de sélection et d'évaluation des candidats, Planview procédera à des vérifications appropriées des antécédents de tous les représentants de Planview susceptibles d'avoir accès aux Données du Client et refusera l'accès aux Données du Client à tout représentant de Planview qui n'aura pas satisfait à cette vérification des antécédents.
- (ii) L'accès aux données est régi par la norme de contrôle d'accès de Planview. Des contrôles sont mis en œuvre pour garantir que l'accès accordé à tous les représentants de Planview est basé sur le principe du moindre privilège et que seuls les représentants de Planview qui ont réellement besoin de connaître ces informations auront accès aux Données du Client, y compris, mais sans s'y limiter, l'utilisation d'un processus formel de gestion des accès pour demander, examiner, approuver, fournir et révoquer cet accès ;
- (iii) Tous les représentants de Planview ayant accès aux Données du Client suivront une formation adéquate sur la protection et le traitement des Données du Client ;
- (iv) Planview maintiendra une politique et un processus disciplinaires qui seront appliqués lorsque des représentants de Planview enfreindront une politique de sécurité ou de confidentialité de Planview ou accéderont aux Données du Client sans autorisation préalable ;
- (v) L'accès au code source de Planview doit être limité et contrôlé afin de ne permettre l'accès qu'aux représentants Planview autorisés ; et
- (vi) Un processus de séparation des tâches sera mis en place afin d'empêcher qu'un seul représentant de Planview ne contrôle tous les aspects clés d'une transaction ou d'un processus commercial critique lié aux données ou aux systèmes du Client.

#### 4. Authentification et Gestion des Accès

Planview fournira des méthodes d'authentification et de contrôle d'accès robustes pour protéger les Données du Client, y compris, mais sans s'y limiter, (i) des mots de passe complexes d'au moins huit caractères ; (ii) une durée de vie maximale de 90 jours pour les mots de passe ; (iii) des identifiants utilisateur uniques ; (iv) une configuration de délai d'expiration de session, et/ou (v) une authentification multifactorielle.

#### 5. Gestion des Changements

Les procédures opérationnelles doivent être documentées et gérées par un processus de contrôle des changements. Planview disposera et maintiendra des politiques et procédures écrites pour examiner, tester et approuver (le cas échéant) les changements affectant l'infrastructure et les systèmes Planview qui traitent les Données du Client. Des critères d'acceptation pour les nouveaux systèmes d'information, les mises à niveau et les nouvelles versions doivent être établis, et des tests appropriés du ou des systèmes doivent être effectués pendant le développement et avant l'acceptation.

#### 6. Continuité des Activités et Reprise Après Sinistre

Planview doit disposer et maintenir des plans écrits de continuité des activités et de reprise après sinistre, qui sont testés/révisés au moins une fois par an.

#### 7. Suppression Sécurisée des Données

Planview mettra en place un processus de destruction et de suppression sécurisées des Données du Client afin de garantir que les Données du Client supprimées ne puissent être lues ou reconstituées de manière pratique.

#### 8. Gestion des Vulnérabilités

Planview mettra en place et maintiendra les processus de gestion des vulnérabilités suivants pour tous les appareils utilisés pour se connecter au réseau et aux services Planview :

- (i) Analyse et Correction de la Configuration : Planview s'alignera sur les meilleures pratiques du secteur en matière de développement, de minimisation des services et de configuration sécurisée des applications Planview ;
- (ii) Analyse et Correction des Vulnérabilités : Planview mettra en œuvre un système d'analyse et de gestion afin d'analyser le réseau, les systèmes et les applications de Planview à la recherche de vulnérabilités ; Planview analysera régulièrement les vulnérabilités et corrigera les vulnérabilités détectées pour les composants dans les environnements de production ;
- (iii) Codage Sécurisé : Planview doit respecter les meilleures pratiques en matière de développement sécurisé pour le développement et le test de tous les codes, API et applications déployés et mis en œuvre à l'appui des Services, y compris, mais sans s'y limiter, les tests de sécurité ou l'analyse des codes achetés ou sous-traités destinés à être utilisés dans les Services ; et
- (iv) Identification des Menaces Malveillantes : Planview disposera et maintiendra des solutions permettant d'identifier et d'empêcher les attaquants malveillants ou les codes malveillants d'accéder ou de compromettre les Données du Client ou les systèmes qui traitent les Données du Client.

Les exceptions aux contrôles de gestion des vulnérabilités doivent être documentées et atténuées sur la base de contrôles de processus métier définis.

#### 9. Réponse aux Incidents de Sécurité

Planview s'engage à :

- (i) Maintenir un plan, des procédures et des moyens de réponse aux incidents de sécurité conformes aux normes de l'industrie.
- (ii) Informer le Client sans délai dès que Planview confirme tout incident connu lié aux données ou toute intrusion malveillante impliquant les données ou les Services utilisés par le Client ;
- (iii) Coopérer avec le Client pour enquêter sur l'incident lié aux données, y remédier et atténuer tout risque supplémentaire pour les Données du Client ou pour les personnes concernées, dans la mesure où cette coopération n'interfère pas avec l'enquête et la résolution de l'incident par Planview ;
- (iv) Fournir une assistance au Client, y compris, le cas échéant, mettre à la disposition du Client les enregistrements, journaux, fichiers, rapports de données et autres documents pertinents nécessaires pour se conformer à la législation ou à la réglementation applicable, comme raisonnablement exigé par le Client, sous réserve des restrictions de confidentialité imposées par des tiers, aux frais exclusifs de Planview ; et
- (v) Conserver les preuves dans la mesure du possible et coopérer avec le Client et les autorités judiciaires, le cas échéant, pendant l'enquête sur l'incident ou la citation à comparaître relative aux Données du Client, y compris l'accessibilité des informations pour les affaires judiciaires, la conservation, la disponibilité et la surveillance.

## Accord sur la confidentialité, la sécurité et le traitement des données (« DPA »)

### 10. Examens de Sécurité

Planview procédera à des examens réguliers de ses Mesures de Sécurité afin de s'assurer qu'elles restent efficaces et appropriées pour protéger les Données du Client, et qu'elles sont conformes aux normes, lois et réglementations applicables dans le secteur. Les risques détectés lors des examens réguliers seront atténués par Planview en temps opportun.

Lors de la mise en œuvre, de la révision et de la mise à jour de ses mesures et politiques de sécurité, Planview tiendra compte :

- (i) Les informations disponibles provenant des activités existantes de Planview en matière de vulnérabilité, de correction, d'audits ou d'incidents ;
- (ii) La nature changeante des menaces, des exploits et des incidents réels liés à la compromission des informations hébergées sur des plateformes informatiques connectées ;
- (iii) La nature confidentielle des Données du Client et les dommages potentiels qui pourraient résulter d'un traitement, d'une perte, d'un accès, d'une détérioration ou d'une destruction accidentels, non autorisés ou illégaux de ces informations ;
- (iv) Les moyens disponibles et émergents permettant de détecter les activités malveillantes et de les rendre moins efficaces ou inefficaces ; et
- (v) L'état du développement technologique et le coût de la mise en œuvre de ces mesures.

### 11. Chiffrement

Planview a mis en place et maintiendra : (i) des méthodes établies pour crypter les Données du Client en transit et au repos ; et (ii) des méthodes établies pour stocker les mots de passe en toute sécurité, conformément aux pratiques standard du secteur.

### 12. Transfert de Supports

Lorsque le transfert physique de supports est autorisé, Planview doit transporter les supports physiques contenant des PII dans des conteneurs scellés avec une chaîne de contrôle documentée.

### 13. Sécurité des Réseaux et des Systèmes

- (i) Les segments de réseau connectés à Internet doivent être protégés par des pare-feu configurés pour protéger tous les appareils qui se trouvent derrière eux et traiter correctement les problèmes de sécurité connus conformément aux meilleures pratiques du secteur ; les pare-feu doivent refuser tout trafic réseau autre que celui autorisé pour les fonctionnalités commerciales ;
- (ii) Planview doit maintenir la capacité de détecter de manière raisonnable une attaque hostile potentielle ;
- (iii) Planview doit disposer de moyens définis pour sécuriser et maintenir la confidentialité, l'intégrité et la disponibilité des configurations système des ordinateurs et des appareils réseau sur le réseau.
- (iv) Les environnements de développement et de production doivent être séparés afin de réduire les risques d'accès non autorisé ou de modifications du système opérationnel.
- (v) Des contrôles de validation doivent être intégrés aux applications afin de détecter toute corruption d'informations due à des erreurs de traitement ou à des actes délibérés ; et
- (vi) Planview doit utiliser une source de temps externe fiable et sûre pour synchroniser les horloges internes du système.

### 14. Capacités du Système et de Journalisation

Planview maintiendra le matériel, les logiciels et/ou les mécanismes procéduraux qui enregistrent, examinent et alertent (lorsqu'un événement de sécurité est détecté) les activités dans les systèmes d'information qui traitent ou accèdent aux Données du Client, y compris les journaux appropriés et les rapports automatisés. Les journaux doivent être conservés afin de faciliter les enquêtes et la surveillance du contrôle d'accès, y compris, mais sans s'y limiter, l'accès et les activités des utilisateurs finaux et les événements liés à la sécurité des informations.

### 15. Programme de Conformité

Planview maintiendra un programme de conformité comprenant des audits et/ou des certifications indépendants réalisés par des tiers, tels que le rapport SOC2 Type II, le certificat ISO 27001 ou tout autre certificat équivalent, et mettra à la disposition du Client, sur demande écrite, des copies de la version la plus récente des certifications ou rapports tiers relatifs aux Services achetés par le Client.

### 16. Protection des Données dès la Conception

Planview intégrera les principes de protection des données dès la conception et de protection des données par défaut dans ses processus, services et systèmes dès le stade le plus précoce et tout au long du cycle de vie des activités de traitement.