POLITIQUE RELATIVE AU TRAITEMENT DES DONNÉES

La présente Politique relative au traitement des données (y compris ses Annexes) (ci-après dénommée la « **Politique** ») fait partie de la Commande et est soumise aux conditions et modalités applicables à la Commande (y compris les Conditions régissant ladite Commande) (ci-après dénommées le « **Contrat** »), telle que conclue entre le Fournisseur et le client signataire du Contrat (ci-après dénommé le « **Client** ») agissant en son propre nom et pour le compte de toute Société liée du Client, et est intégrée aux présentes par renvoi.

La présente Politique remplace, dans leur intégralité, l'ensemble des contrats, politiques, annexes, ou autres documents existants applicables au traitement et à la protection des Données à caractère personnel du Client dans le cadre des Services.

Les termes définis dans le Contrat et qui sont utilisés dans la présente Politique sans être définis à nouveau ont le sens qui leur est attribué dans le Contrat. À l'exception des modifications définies ci-après, les conditions du Contrat restent en vigueur et conservent leur plein effet.

La présente Politique reflète l'engagement des parties à respecter les Lois relatives à la protection des données en ce qui concerne le Traitement des Données à caractère personnel du Client dans le cadre des Services prévus au Contrat. Si et dans la mesure où le libellé de la présente Politique est en contradiction avec le Contrat, la présente Politique prévaudra.

La présente Politique acquiert force obligatoire à la date d'entrée en vigueur du Contrat ou à la date de signature de la présente Politique par les parties si cette date de signature est postérieure à la date d'entrée en vigueur du Contrat.

1. Définitions.

Aux fins de la présente Politique, les définitions suivantes, ainsi que celles incluses dans le corps de la présente Politique, s'appliquent.

a) « **Données à caractère personnel du Client** » désigne les Données à caractère personnel détenues ou contrôlées par le Client, et qui sont fournies par ou au nom du Client au Fournisseur dans le cadre des Services.

b) « **Sous-traitant sous contrat** » désigne le Fournisseur ou un Sous-traitant ultérieur.

c) « **Responsable du traitement** » désigne l'entité qui détermine les finalités et les moyens du Traitement des Données à caractère personnel du Client.

d) « **Lois relatives à la protection des données** » désigne toutes les lois et réglementations applicables au traitement des Données à caractère personnel du Client dans le cadre de la fourniture des Services aux termes du Contrat. Les « Lois relatives à la protection des données » peuvent inclure, sans que cette liste ne soit exhaustive, la Loi californienne sur la protection de la vie privée des consommateurs de 2018 (California Consumer Privacy Act, ci-après la « **CCPA** ») ; le Règlement général sur la protection des données 2016/679 de l'UE (ci-après le « **RGPD** ») et les législations nationales de mise en œuvre correspondantes ; la loi fédérale suisse sur la protection des données ; le Règlement général sur la protection des données du Royaume-Uni (United Kingdom General Data Protection Regulation, ci-après le « **RGPD du Royaume-Uni** ») ; et la Loi britannique sur la protection des données de 2018 (United Kindgom Data Protection Act) (dans chaque cas, tels que modifiés, adoptés ou remplacés à tout moment) ;

e) « **Personne concernée** » a le sens donné à ce terme dans les Lois relatives à la protection des données ;

f) « **Données à caractère personnel** » désigne toute information qui a été fournie par ou au nom du Client pour une utilisation dans les Services et qui se rapporte à une personne identifiée ou identifiable.

g) « **Traiter** » ou « **Traitement** » désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données à caractère personnel du Client ou des ensembles de Données à caractère personnel du Client, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

h) « **Sous-traitant** » désigne l'entité qui traite les Données à caractère personnel du Client pour le compte du Responsable du traitement.

i) « **Incident(s) de sécurité** » désigne la destruction accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux Données à caractère personnel du Client. Ne sont pas incluses dans les Incidents de sécurité les tentatives infructueuses ou les activités qui ne compromettent pas la sécurité des Données personnelles du Client, notamment les tentatives de connexion infructueuses, les pings, les analyses de port, les attaques par déni de service et autres attaques réseau sur les pares-feux ou les systèmes en réseau.

j) « **Services** » désigne les services que le Fournisseur exécute aux termes du Contrat.

k) « **Clauses contractuelles types** » (incorporées ici par renvoi) désigne :

les « Clauses contractuelles types 2021 », définies comme les clauses émises en vertu de la Décision d'exécution (UE) 2021/914 de la Commission européenne de juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil, disponible à l'adresse http://data.europa.eu/eli/dec_impl/2021/914/oj (telles que modifiées et mises à jour à tout moment).

l) « **Sous-traitant(s) ultérieur(s)** » désigne les distributeurs autorisés du Fournisseur et les fournisseurs de services tiers qui Traitent les Données à caractère personnel du Client.

m) « **Autorité de contrôle** » désigne une autorité publique indépendante établie conformément aux Lois relatives à la protection des données pour superviser le respect desdites Lois relatives à la protection des données.

2. Utilisation et Traitement des données.

a) Rôles des parties. Les parties reconnaissent et conviennent que (i) lorsque le Client est un Responsable du traitement, le Fournisseur est le Sous-traitant, et (ii) lorsque le Client est un Sous-traitant, le Fournisseur est un Sous-traitant ultérieur du Client. Par ailleurs, lorsque la CCPA s'applique au Traitement par le Fournisseur de Données à caractère personnel du Client, les parties reconnaissent et conviennent que le Client est une Entreprise (« Business »), au sens donné à ce terme par la CCPA et ses règlements d'applications, et que le Fournisseur est vis-à-vis du Client un Fournisseur de Services (« Service Provider ») au sens donné à ce terme par la CCPA.

b) Instructions documentées. Le Client demande au Fournisseur de Traiter les Données à caractère personnel du Client pour lui permettre de fournir les Services et pour permettre au Client de recevoir les Services conformément au Contrat, à la présente Politique, à tout énoncé de travail applicable et à toute instruction convenue par écrit par les parties. L'objet de ce Traitement est l'utilisation des Services par le Client et ses utilisateurs finaux. Les catégories de Personnes concernées sont les utilisateurs des Services et les occupants des locaux où les Services sont utilisés et peuvent donc inclure les employés et les visiteurs du Client. Le Fournisseur doit s'assurer que tout transfert de Données à caractère personnel du Client hors de l'EEE et/ou du Royaume-Uni est effectué conformément aux Lois relatives à la protection des données, en utilisant un mécanisme de transfert légal. Le Client doit s'assurer que le Traitement des Données à caractère personnel du Client par le Fournisseur, lorsqu'il est effectué conformément aux instructions du Client, n'entraîne pas la violation par le Fournisseur d'une loi ou d'un règlement applicable, y compris les Lois relatives à la protection des données applicables. Le Client est seul responsable de l'exactitude, de la qualité et de la légalité des Données à caractère personnel du Client, de l'ensemble des consentements, processus et notifications nécessaires pour permettre légalement le transfert au Fournisseur des Données à caractère personnel du Client en vertu du Contrat et de la présente Politique, et des moyens utilisés par le Client pour l'acquisition des Données à caractère personnel. La durée pendant laquelle le Fournisseur traite les Données à caractère personnel du Client correspond à la durée du Contrat à laquelle s'ajoute toute durée de conservation applicable au titre de la présente Politique. Sauf interdiction légale, le Fournisseur doit informer le Client par écrit s'il a des motifs raisonnables de croire qu'il existe un conflit entre les instructions du Client et les Lois relatives à la protection des données.

c) Autorisation de faire appel à des sous-traitants ultérieurs. Dans la mesure nécessaire pour remplir les obligations contractuelles du Fournisseur au titre du Contrat, le Client autorise par la présente le Fournisseur à engager des Sous-traitants ultérieurs. La liste actuelle des Sous-traitants ultérieurs du Fournisseur pour les Services applicables est disponible l'adresse www.eptura.com/subprocessors « **Liste des sous-traitants ultérieurs** ». Le Client accepte le choix des Sous-traitants ultérieurs figurant dans la Liste des sous-traitants ultérieurs. Le Fournisseur s'engage à ne pas transférer de Données à caractère personnel à des entités dont le nom ne figure pas sur la Liste des sous-traitants ultérieurs.

d) Fournisseur et conformité des Sous-traitants ultérieurs. Le Fournisseur (i) s'engage à conclure un accord écrit avec les Sous-traitants ultérieurs portant sur le Traitement des Données à caractère personnel du Client par lesdits Sous-traitants ultérieurs qui impose à ces derniers d'appliquer aux Données à caractère personnel du Client des exigences de protection des données compatibles avec celles de la présente Politique ; et (ii) reconnaît rester responsable des actes et omissions de ses Sous-traitants ultérieurs dans la même mesure que s'il réalisait directement les Services confiés à chaque Sous-traitant ultérieur en application de la présente Politique.

e) Droit de s'opposer au recours à des Sous-traitants ultérieurs. Le Fournisseur informe le Client, au moins 15 jours avant la désignation de tout nouveau Sous-traitant ultérieur, de son intention d'engager de nouveaux Sous-traitants ultérieurs en mettant à jour la Liste des sous-traitants ultérieurs et le Fournisseur offre au Client la possibilité de s'inscrire pour recevoir des

notifications desdites modifications. Le Client peut s'opposer à l'utilisation par le Fournisseur du nouveau Sous-traitant ultérieur en notifiant rapidement au Fournisseur par écrit son opposition dans les 15 jours qui suivent la réception de la notification du Fournisseur. La notification au Client est remise à l'adresse ou aux adresses e-mail communiquées dans la Commande de Services ou communiquées au Fournisseur d'une autre manière lors de la souscription des Services. Si le Client ne s'oppose pas à l'engagement du nouveau Sous-traitant ultérieur conformément au présent article, le nouveau Sous-traitant ultérieur est réputé accepté aux fins de la présente Politique. Si le Client s'oppose à la désignation ou au remplacement d'un Sous-traitant ultérieur par le Fournisseur sur la base de motifs raisonnables liés à la protection des données, il doit en informer le Fournisseur par écrit en détaillant cette objection avant la désignation ou le remplacement du Sous-traitant ultérieur. Dans un tel cas, le Fournisseur doit déployer des efforts raisonnables pour fournir les Services au Client conformément au Contrat sans faire appel au Sous-traitant ultérieur. Si le Fournisseur a raisonnablement besoin de recourir au Sous-traitant ultérieur et n'est pas en mesure de satisfaire le Client quant au caractère adéquat du Sous-traitant ultérieur dans les trente (30) jours suivant l'opposition du Client, le Client peut choisir de résilier uniquement la partie des Services ou de la ou des Commande(s) qui ne peut pas être fournie par le Fournisseur sans recourir au Sous-traitant ultérieur auquel il s'est opposé.

f) Confidentialité. Le Fournisseur doit s'assurer que son personnel et celui de ses Sociétés liées engagés dans le Traitement des Données à caractère personnel du Client sont informés de la nature confidentielle des Données à caractère personnel du Client et ont signé des accords de confidentialité écrits.

g) Analyse d'impact relative à la protection des données et consultation préalable. Le Fournisseur doit prêter raisonnablement assistance au Client pour toute évaluation d'impact sur la protection des données (aux frais du Client uniquement dans le cas où une telle coopération raisonnable nécessite du Fournisseur l'affectation de ressources importantes à cet effet) et pour les consultations préalables avec toute Autorité de contrôle ou autre autorité compétente en matière de confidentialité des données dans la mesure où cela est requis par les Lois relatives à la protection des données applicables, uniquement, dans chacun des cas, dans le cadre du Traitement des Données à caractère personnel du Client, et en tenant compte de la nature du Traitement et des informations à la disposition du Fournisseur.

3. Personnes concernées.

Le Fournisseur doit, dans les limites autorisées par les Lois relatives à la protection des données, informer le Client si le Fournisseur reçoit une demande d'une Personne concernée qui cible les Données à caractère personnel du Client ou qui cible autrement le Client, y compris lorsque la Personne concernée souhaite exercer l'un de ses droits en vertu des Lois relatives à la protection des données (ces différentes demandes étant dénommées ci-après « **Demande de personne concernée** »). Si le Fournisseur reçoit une Demande de personne concernée en lien avec les Données à caractère personnel du Client, le Fournisseur doit conseiller à la Personne concernée de soumettre sa demande au Client et le Client est tenu de répondre à ladite demande, y compris, le cas échéant, en utilisant les fonctionnalités des Services. Dans la mesure où le Client n'est pas en mesure d'accéder à ses Données à caractère personnel dans le cadre des services, en utilisant les contrôles adéquats ou autrement, le Fournisseur (sur demande écrite du Client et en tenant compte de la nature du Traitement) apporte sa coopération raisonnable d'un point de vue commercial pour aider le Client à répondre aux Demandes de la personne concernée.

4. Transferts de données.

Si des Données à caractère personnel du Client provenant de l'Espace économique européen, de la Suisse et/ou du Royaume-Uni sont transférées par le Client au Fournisseur dans un pays qui n'a pas été considéré comme offrant un niveau de protection adéquat en vertu des Lois relatives à la protection des données applicables, les parties conviennent que le transfert doit être régi par les Clauses contractuelles types (ou « CCT »). Lorsque les CCT sont applicables et que le Client agit en qualité de Responsable du traitement des Données à caractère personnel du Client, tandis que le Fournisseur agit en qualité de Sous-traitant des Données à caractère personnel du Client, chacune des parties doit se conformer à ses obligations en application du Module 2 des CCT. Lorsque les CCT sont applicables et que le Client et le Fournisseur agissent tous deux en qualité de Sous-traitant des Données à caractère personnel du Client, chacune des parties doit se conformer à ses obligations en application du Module 3 des CCT. Les parties conviennent que : (i) la clause d'adhésion facultative prévue par la Clause 7 ne s'applique pas ; (ii) l'attestation de suppression requise par les Clauses 8.5 et 16(d) des CCT est fournie sur demande écrite du Client ; (iii) les mesures que le Fournisseur est tenu de prendre aux termes de la Clause 8.6(c) des CCT ne couvrent que les systèmes impactés du Fournisseur ; (iv) l'audit décrit à la Clause 8.9 des CCT doit être effectué conformément à l'article 7 de la présente Politique ;

(v) dans la Clause 9, le délai minimum de notification préalable des changements de Sous-traitant ultérieur est celui indiqué à l'article 2(e) de la présente Politique ; (vi) lorsque les Lois relatives à la protection des données le permettent, le Fournisseur peut engager des Sous-traitants ultérieurs existants en utilisant la décision de la Commission européenne C(2010)593 relatives aux CCT entre Sous-traitants et Responsables du traitement et ce recours aux Sous-traitants ultérieurs est réputé conforme à la Clause 9 des CCT ; (vii) dans la Clause 11, le libellé facultatif ne s'applique pas ; (viii) le droit de résiliation prévu par la Clause 14(f) et la Clause 16(c) des CCT est limité à la résiliation des CCT, auquel cas le Traitement correspondant des Données à caractère personnel du Client affectées par cette résiliation doit être interrompu, sauf accord contraire entre les parties ; (ix) les informations requises au titre de la Clause 15.1(c) sont fournies sur demande écrite du Client ; (x) dans la Clause 17, les clauses convenues entre les Parties sont régies par les lois de la République d'Irlande ; (xi) dans la Clause 18(b), les litiges sont tranchés devant les tribunaux de la République d'Irlande ; (xii) l'Annexe A de la présente Politique contient les informations requises à l'annexe I des CCT ; (xiii) l'Annexe B de la présente Politique contient les informations requises à l'annexe II des CCT ; (xiv) dans la mesure où des Données personnelles sont soumises aux Lois britanniques sur la confidentialité des données, les CCT sont complétées par l'Annexe C ; et (xv) nonobstant toute disposition contraire, le Client rembourse au Fournisseur l'ensemble des coûts et dépenses engagés par le Fournisseur dans le cadre de l'exécution des obligations du Fournisseur au titre des Clauses 15.1(b) et 15.2 des CCT. La signature de la présente Politique par chacune des parties est considérée comme une signature des CCT dans la mesure où les CCT s'appliquent aux termes des présentes.

5. Programme de sécurité de l'information.

Le Fournisseur a mis en place et s'engage à maintenir des mesures administratives, techniques et organisationnelles appropriées pour protéger les Données à caractère personnel du Client contre un Incident de sécurité, compte tenu de l'état du développement technologique et du coût de la mise en œuvre de ces mesures, ainsi que de la nature, de la portée, du contexte et des finalités du Traitement et de la probabilité et de la gravité de l'atteinte aux intérêts des Personnes concernées susceptible de résulter d'un tel Incident de sécurité (y compris, le cas échéant, les mesures visées à l'article 32(1), du RGPD). Toutes les questions sur les pratiques de sécurité du Fournisseur peuvent être envoyées à l'équipe Sécurité et confidentialité du à l'adresse privacy@eptura.com.

6. Incidents de sécurité.

a) Le Fournisseur adresse une notification écrite au Client dans les meilleurs délais lorsqu'il apprend l'existence d'un Incident de sécurité. Une telle notification ne constitue pas une reconnaissance de faute ou de responsabilité. La notification doit, dans la mesure du possible, permettre au Client d'informer les Personnes concernées par l'Incident de sécurité aux termes des Lois relatives à la protection des données et, dans la limite des connaissances du Fournisseur, (i) décrire la nature de l'Incident de sécurité, y compris, si possible, les catégories et le nombre approximatif de Personnes concernées, ainsi que les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ; et (ii) décrire les mesures prises ou proposées par le Fournisseur pour traiter l'Incident de sécurité, y compris, le cas échéant, les mesures d'atténuation.

b) En cas d'Incident de sécurité et avant d'effectuer toute déclaration publique ou toute notification obligatoire, le Fournisseur s'engage à demander l'approbation du Client avant toute notification aux Personnes concernées affectées ou aux Autorités de contrôles concernant l'Incident de sécurité. Nonobstant la phrase précédente, le Client ne peut être tenu d'aller à l'encontre de ses obligations au titre des Lois relatives à la protection des données.

c) Les obligations décrites aux articles 7(a) et 7(b) ne s'appliquent pas dans le cas où une violation des Données à caractère personnel résulte d'actions ou d'omissions du Client.

7. Audits.

a) Le Fournisseur fait appel à des auditeurs tiers indépendants pour vérifier le caractère adéquat du Traitement des Données à caractère personnel du Client. Cet audit : (i) est exécuté au moins une fois par an ; (ii) est exécuté par un professionnel qualifié au choix et aux frais du Fournisseur ; et (iii) démontre le respect par le Fournisseur des normes de sécurité des données en vigueur applicables au Traitement des Données à caractère personnel (le rapport d'audit est dénommé ci-après le « **Rapport** »). Sur demande écrite du Client, le Fournisseur remet au Client un résumé de son Rapport afin que le Client puisse vérifier de manière raisonnable le respect par le Fournisseur des obligations de sécurité prévues par la présente Politique. Toutes les dispositions dudit Rapport sont soumises à des procédures raisonnables de confidentialité.

b) Si le Fournisseur n'est pas en mesure de fournir rapidement les Rapports actuels, le Client peut, sur demande écrite, exécuter (à ses propres frais) un audit de vérification de la sécurité de l'information. Un tel audit est soumis aux conditions suivantes : (i) Le Client doit informer au moins trente (30) jours à l'avance de son

intention d'effectuer un audit ; (ii) au plus tard deux (2) semaines avant l'activité d'audit, la portée et le calendrier de l'audit doivent être convenus d'un commun accord ; (iii) tout auditeur indépendant est tenu de signer un accord de confidentialité raisonnablement exigé par le Fournisseur avant l'audit ; (iv) l'audit doit être effectué pendant les heures de travail normales du Fournisseur ; (v) l'audit doit être achevé en un (1) jour ouvré ; (vi) le droit de procéder à l'audit comprend le droit d'inspecter, mais pas de copier ni de supprimer un enregistrement, à l'exception de ceux qui concernent spécifiquement et exclusivement le Client ; et (vii) l'audit ne doit pas inclure de tests d'intrusion, d'analyses de vulnérabilité ou autres tests de sécurité. Le Client ne peut pas exercer son droit d'effectuer un audit plus d'une fois par période de douze (12) mois ; toutefois, le Client peut effectuer des audits supplémentaires en cas (i) d'Incident de sécurité impliquant des Données à caractère personnel du Client ; ou (ii) de demande d'une Autorité de surveillance ou de toute autre autorité de réglementation semblable chargée de l'application des Lois relatives à la protection des données dans tout pays ou territoire. Une réunion est organisée entre le Fournisseur et le Client pour discuter des résultats de l'audit ; les mesures correctives et les délais sont déterminés par le Fournisseur à sa seule discrétion.

8. Suppression de données.

Le Fournisseur doit mettre les Données personnelles du Client à la disposition du Client pour exportation sur demande écrite effectuée dans les trente (30) jours suivant la date de résiliation/d'expiration du Contrat. Par la suite, le Fournisseur supprime dans un délai de soixante (60) jours toutes les Données personnelles du Client (à l'exclusion de toutes les copies de sauvegarde ou d'archivage qui doivent être supprimées conformément à la politique de conservation des données du Fournisseur), sauf lorsque le Fournisseur est tenu de conserver des copies en application des Lois relatives à la protection des données, auquel cas le Fournisseur protège ces Données à caractère personnel du Client contre tout Traitement ultérieur. Lorsque le Client demande une copie de ses Données à caractère personnel, le Fournisseur doit satisfaire à ladite demande dans un délai de 45 jours à compter de la date de la demande.

9. Responsabilité.

La présente Politique s'applique sans préjudice des droits et obligations des parties au titre du Contrat, qui reste en vigueur et pleinement applicable, notamment en ce qui concerne les limitations et exclusions de responsabilité qui y figurent et qui s'appliquent à la présente Politique comme si elles y figuraient intégralement. En cas de conflit entre les dispositions de la présente Politique et les dispositions du Contrat, les dispositions de la présente Politique prévalent dans la mesure où il est question du traitement des Données à caractère personnel du Client.

10. Dispositions diverses.

a) La présente Politique est régie et interprétée conformément à la loi et aux règles de compétence du pays ou du territoire qui régissent le Contrat, sauf indication contraire dans la présente Politique ou lorsque les Lois relatives à la protection des données l'exigent.

b) Le Fournisseur peut modifier les conditions de la présente Politique lorsque les modifications apportées (a) sont nécessaires pour se conformer aux Lois relatives à la protection des données, à la réglementation applicable, à une décision d'un tribunal ou à des directives émises par une autorité de régulation ou un organisme public ; ou (b) n'ont pas d'impact négatif important sur les droits du Client au titre de la Politique. Le Fournisseur doit donner un préavis d'au moins trente (30) jours avant d'effectuer une modification importante des dispositions de la présente Politique. Si les modifications ont un impact important sur l'utilisation des Services par le Client, ce dernier a le droit de résilier les Services concernés dans les trente (30) jours suivant la réception d'une notification écrite l'informant des modifications.

Annexe A

ANNEXE I DES CLAUSES CONTRACTUELLES TYPES

A. **LISTE DES PARTIES**

MODULE 2 : Transfert de responsable du traitement à sous-traitant

MODULE 3 : Transfert de sous-traitant à sous-traitant

Exportateur(s) de données :

Nom :	Le Client identifié dans le Contrat et/ou le(s) Bon(s) de commande/Énoncé(s) des travaux et toutes les Sociétés liées du Client
Adresse :	Adresse du Client, telle qu'identifiée dans le Contrat et/ou le(s) Bon(s) de commande/Énoncé(s) des travaux
Personne de contact :	Adresse e-mail du Client, telle qu'identifiée dans le Contrat et/ou le(s) Bon(s) de commande/Énoncé(s) des travaux
Activités en rapport avec les données transférées :	Souscription de Services auprès du Fournisseur
Rôle :	Responsable du traitement (module 2) ; Sous-traitant (module 3)

Importateur(s) de données :

Nom :	Le Fournisseur identifié dans le Contrat et/ou le(s) Commande(s)/Énoncé(s) des travaux et toutes les Sociétés liées du Client
Adresse :	Adresse du Fournisseur, telle qu'identifiée dans le Contrat et/ou le(s) Commandes/Énoncé(s) des travaux
Personne de contact :	privacy@eptura.com
Activités en rapport avec les données transférées :	Le Fournisseur est un fournisseur d'espace de travail cloud d'entreprise et de solutions de gestion des actifs, qui Traite les Données à caractère personnel du Client selon les instructions de l'Exportateur de données conformément aux modalités du Contrat et de la Politique.
Rôle :	Sous-traitant

B. DESCRIPTION DU TRANSFERT

MODULE 2 : Transfert de responsable du traitement à sous-traitant

MODULE 3 : Transfert de sous-traitant à sous-traitant

Objet du traitement :	L'objet du Traitement des Données à caractère personnel par le Fournisseur est la fourniture de services à l'Exportateur de données conformément au Contrat.
Nature et finalités du Traitement :	Le Traitement est lié à la fourniture de solutions SaaS au Client, comme indiqué de façon plus détaillée dans le Contrat, et le Fournisseur et ses Sous-traitants ultérieurs effectuent les opérations de Traitement des Données personnelles nécessaires à la fourniture de ces services conformément aux instructions de l'Exportateur de données, y compris, mais pas uniquement la transmission, le stockage et tout autre traitement des Données à caractère personnel fournies pour les Services.
Durée du Traitement :	Le Fournisseur traite les Données à caractère personnel au nom de l'Exportateur de données jusqu'à ce que l'Exportateur de données cesse d'utiliser les Services.

Catégories de personnes concernées :	Personnes concernées dont les Données personnelles du Client sont traitées conformément au Contrat.
Catégories de Données à caractère personnel :	Données personnelles du Client traitées conformément au Contrat.
Catégories particulières de Données à caractère personnel :	Le traitement des Catégories particulières de Données à caractère personnel n'est pas autorisé dans les Services.
Objet, nature et durée du traitement par les Sous-traitants ultérieurs :	Tout transfert à des Sous-traitant ultérieurs a pour but l'exécution des Services conformément au Contrat.

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

MODULE 2 : Transfert de responsable du traitement à sous-traitant

MODULE 3 : Transfert de sous-traitant à sous-traitant

L'autorité de contrôle compétente est celle mandatée par la Clause 13 des CCT. Si aucune autorité de contrôle n'est mandatée par la Clause 13, l'autorité compétente est la Commission irlandaise de protection des données (Data Protection Commission, ou DPC) et si cela n'est pas possible, l'autorité convenue entre les parties dans le respect des conditions stipulées à la Clause 13.

Annexe B

ANNEXE II DES CLAUSES CONTRACTUELLES TYPES

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

MODULE 2 : Transfert de responsable du traitement à sous-traitant

MODULE 3 : Transfert de sous-traitant à sous-traitant

Description des mesures techniques et organisationnelles mises en œuvre par le ou les importateur(s) 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.

Pour déterminer les mesures de sécurité techniques et organisationnelles (ci-après dénommées « Normes de sécurité ») requises aux termes du Contrat, le Fournisseur tient compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des différents degrés de probabilité et de sévérité des risques pour les droits et libertés des personnes physiques. Le Fournisseur doit maintenir des procédures pour tester, analyser et évaluer régulièrement l'efficacité des Normes de sécurité afin de garantir la sécurité du traitement des Données à caractère personnel du Client.

Le Fournisseur convient de ce qui suit quant aux Données à caractère personnel du Client :

1. Garanties – Programme. Le Fournisseur met en œuvre des garanties appropriées, conformes aux normes du secteur, conçues pour protéger les Données à caractère personnel du Client, en préservant leur confidentialité, leur intégrité et leur disponibilité. Le Fournisseur s'assure que toutes ces garanties sont conformes aux Lois applicables et au Contrat, y compris, le cas échéant, la Politique relative au traitement des données (PTD).

2. Garanties – détails. Au minimum, les Normes de sécurité du Fournisseur doivent inclure : (a) la sécurisation des installations, des centres de données, des fichiers papier, des serveurs, des systèmes de sauvegarde et des équipements informatiques, y compris, mais pas uniquement, tous les appareils mobiles et autres équipements dotés d'une capacité de stockage d'informations ; (b) la sécurité du réseau, des applications des appareils, des bases de données et des plateformes ; (c) la sécurisation de la transmission, du stockage et de l'élimination des données ; (d) l'authentification et les contrôles d'accès au sein des applications, des systèmes d'exploitation et des équipements ; (e) la tenue de registres d'accès au matériel et la conservation de ces registres de contrôle d'accès pendant une période suffisante pour permettre une enquête ; (f) le chiffrement des Données à caractère personnel du Client au repos, y compris lorsqu'elles sont stockées sur un agenda électronique, un disque dur portable ou un support électronique amovible doté d'une capacité de stockage d'informations ; (g) le chiffrement des Données à caractère personnel du Client lorsqu'elles sont transmises sur des réseaux publics ou sans fil ; (h) la séparation des Données à caractère personnel du Client et des informations des autres clients du Fournisseur ; (i) la sécurité et l'intégrité du personnel, y compris, mais sans s'y limiter, la vérification des antécédents conformément à la loi applicable ; (j) des tests annuels externes et internes et des analyses de vulnérabilité ainsi que la mise en œuvre rapide, aux frais exclusifs du Fournisseur, d'un plan de mesures correctives (y compris un calendrier) pour corriger les problèmes importants identifiés lors des tests ; et (k) la limitation de l'accès aux Données à caractère personnel du Client et la fourniture d'une formation sur la confidentialité et la sécurité des informations au Personnel autorisé du Fournisseur. « Personnel autorisé » désigne le personnel du Fournisseur qui a besoin de connaître ou d'accéder autrement aux données du client pour permettre au Fournisseur de s'acquitter de ses obligations aux termes du Contrat, et qui est lié par des obligations de confidentialité écrites suffisantes pour protéger les Données à caractère personnel du Client conformément aux termes du Contrat, y compris, le cas échéant, la PTD.

3. Logiciels malveillants. Le logiciel du fournisseur tel qu'il est livré ne contient aucun virus, logiciel malveillant, rançongiciel, enregistreur de frappe, aucune bombe logique, aucun cheval de Troie, ver ou autres routines logicielles conçues pour désactiver, effacer ou endommager de toute autre façon les logiciels, le matériel ou les données détenues ou contrôlées par le Client.

4. Matériel ou équipement interdit. Le Fournisseur ne peut pas utiliser de matériel ou d'équipements non conformes à l'Article 889(a)(1)(B) de la Loi de finances relative au budget de défense nationale des États-Unis (National Defense Authorization Act) pour l'exercice 2019. Le Fournisseur fournit une déclaration de conformité à cette disposition sur demande. Si le Fournisseur ne peut plus se conformer à cette disposition, le Fournisseur en informe immédiatement le Client par l'envoi d'un e-mail à la personne de contact de sécurité communiquée.

5. Reprise après sinistre et continuité des activités. Le Fournisseur maintient et met en œuvre un plan de continuité et de reprise des activités (ci-après dénommé « PCRA ») qui comprend au moins : (a) la documentation des processus opérationnels, procédures et responsabilités applicables ; (b) la méthodologie de sauvegarde ; (c) l'identification des scénarios de reprise après sinistre et des accords de niveau de service relatifs à la reprise du service ; (d) les responsabilités des Sous-traitants ultérieurs en cas de sinistre ; (e) une stratégie de communication ; et (f) les procédures de retour au service normal. Le PCRA doit être révisé tous les ans. Le Fournisseur doit s'assurer qu'il est en mesure de mettre en œuvre le PCRA à tout moment conformément à ses dispositions. Le Fournisseur doit tester le PCRA régulièrement (et dans tous cas, au moins une fois par an). Sur demande, le Fournisseur doit envoyer un rapport écrit résumant les résultats du test le plus récent et doit mettre en œuvre rapidement toutes les actions ou mesures correctives dont la nécessité a été convenue mutuellement par les parties à la suite de ces tests.

6. Incidents de sécurité. Lorsque le Fournisseur découvre ou soupçonne raisonnablement l'existence de (i) tout accès non autorisé aux Données client ou divulgation non autorisée de Données client ; (ii) tout accès non autorisé aux applications ou aux systèmes détenus, gérés ou sous-traités par le Fournisseur (ci-après dénommés « Systèmes du Fournisseur ») sur lesquels les Données à caractère personnel du Client sont traitées (chacun de ces accès étant dénommé ci-après un « Incident de sécurité »), le Fournisseur doit, rapidement et dans les meilleurs délais :

(i) prendre des mesures d'atténuation et/ou de remédiation des Incidents de sécurité afin de protéger les Données à caractère personnel du Client contre des risques et dommages supplémentaires, et lancer une enquête ;

(ii) instaurer des contrôles appropriés pour maintenir et préserver toutes les preuves électroniques se rapportant à l'Incident de sécurité conformément aux normes du secteur ;

(iii) signaler la nature de l'Incident de sécurité au Client (y compris, si possible, les catégories de données violées et les catégories de méthodes de perte de données, et dans la mesure où des Données à caractère personnel du Client sont touchées, les catégories et le nombre approximatif de personnes concernées et le nombre approximatif d'enregistrements de Données à caractère personnel du Client concernés) ;

(iv) indiquer le nom et les coordonnées de la personne de contact du Fournisseur susceptible de fournir de plus amples informations, les conséquences probables de l'Incident de sécurité, si elles sont connues, et les mesures prises ou proposées pour résoudre l'Incident de sécurité, y compris (le cas échéant) des mesures visant à en atténuer les effets négatifs potentiels ;

(v) prendre des mesures pour prévenir la survenance de tout Incident semblable à l'avenir. Pour éviter toute ambiguïté, il est précisé que le Fournisseur n'est pas tenu de signaler les pings sur les pares-feux, les analyses de port ni les logiciels malveillants qui sont très peu susceptibles d'entraîner un accès non autorisé à des informations, une utilisation, une divulgation, une modification, une destruction non autorisée d'informations ou une interférence avec les systèmes du Fournisseur, qui ne doivent pas être considérés comme des Incidents de sécurité que le Fournisseur doit signaler au Client ; et

(vi) participer et coopérer aux investigations, litiges, enquêtes, réclamations, actions en justices ou actions réglementaires découlant d'un Incident de sécurité.

7. Certifications et évaluations de sécurité. Le Fournisseur doit engager des sociétés tierces d'évaluation de la sécurité (audit) pour effectuer annuellement des audits de certification et des tests de sécurité. À la demande du Client, le fournisseur doit fournir au client la preuve de la certification et des tests courants, y compris les certificats, les résumés et autres documents jugés pertinents à la seule, mais raisonnable, discrétion du Fournisseur (ci-après dénommés les « Dossiers d'évaluation ») pour démontrer sa conformité au regard du Contrat et des Lois.

8. Questionnaires de sécurité. Le Fournisseur doit répondre, une fois par période de douze (12) mois au maximum et sur demande, à un questionnaire de fournisseur de services de cybersécurité ou à une enquête comparable, de longueur raisonnable, et qui ne nécessite pas la production de preuves justificatives autres que les Dossiers d'évaluation courants.

Assistance aux demandes des Personnes concernées. Le Client est responsable de la communication avec les Personnes concernées conformément à la Clause 15.1(a) des CCT.

Annexe C

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

TABLE 1: PARTIES

Start date	The date on which the Customer or its Affiliate identified in the Agreement and/or Order Form(s)/Statement(s) of Work enters into the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: The Customer identified in the Agreement and/or Order Form(s)/Statement(s) of Work and all Affiliates of Customer Trading name (if different): Main address (if a company registered address): Customer's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work Official registration number (if any) (company number or similar identifier): The registered number of the Customer or Affiliate of the Customer identified in the Agreement and/or Order Form(s)/Statement(s) of Work	Full legal name: The Provider identified in the Agreement and/or Order Form(s)/Statement(s) of Work Trading name (if different): Main address (if a company registered address): Provider's address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work Official registration number (if any) (company number or similar identifier): The registered number of the Provider identified in the Agreement and/or Order Form(s)/Statement(s) of Work
Key Contact	Contact details including email: Customer's email address, as identified in the Agreement and/or Order Form(s)/Statement(s) of Work	Full Name (optional): James Carder Job Title: Chief Information Security Officer Contact details including email: privacy@eptura.com
Signature (if required for the purposes of Section 2)	Not required	Not required

TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date:

	Reference (if any): Other identifier (if any): Or x the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	x			General Authorisation	14 days	
3	x			General Authorisation	14 days	
4						

TABLE 3: APPENDIX INFORMATION

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As identified in Exhibit A
Annex 1B: Description of Transfer: As identified in Exhibit A
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As identified in Exhibit B
Annex III: List of Sub processors (Modules 2 and 3 only): See www.eptura.com/subprocessors

TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☐ Importer x Exporter ☐ neither Party

PART 2: MANDATORY CLAUSES

ENTERING INTO THIS ADDENDUM

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

INTERPRETATION OF THIS ADDENDUM

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section **Error! Reference source not found.**.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

HIERARCHY

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

INCORPORATION OF AND CHANGES TO THE EU SCCS

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

AMENDMENTS TO THIS ADDENDUM

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which: a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or b. reflects changes to UK Data Protection Laws; The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in: a its direct costs of performing its obligations under the Addendum; and/or b its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.