

**1. OBJET DE SES CONDITIONS DE TRAITEMENT DE DONNEES**

- 1.1 Le Client ci-après dénommé (le “**Responsable de Traitement**”) est le responsable de traitement, qui détermine les finalités pour lesquelles et la façon avec laquelle les Données à Caractère Personnel relatives à une Personne Concernée sont ou doivent être Traitées.
- 1.2 Unit4 et ses filiales ci-après dénommées le (« **Sous-Traitant** ») est le sous-traitant, qui agit pour le compte du Responsable de Traitement sans être subordonné à son autorité directe.
- 1.3 Le Sous-Traitant Traitera les Données à Caractère Personnel pour le compte du Responsable de Traitement (et le Responsable de Traitement y consent) conformément au droit applicable et aux présentes Conditions de Traitement de Données, y compris toutes ses annexes.
- 1.4 L'Annexe 1 décrit sans limitation les finalités et les moyens du Traitement, les catégories de Données à Caractère Personnel qui feront l'objet d'un Traitement et la période de rétention desdites Données à Caractère Personnel et les pays (ou lieu(x)) où les Données à Caractère Personnel seront Traitées.
- 1.5 L'Annexe 2 décrit les Mesures de Sécurité applicables adoptées par le Sous-Traitant, que le Responsable de Traitement confirme être adéquates.
- 1.6 L'Annexe 3 décrit les coordonnées de tout Sous-Traitant Ultérieurs.
- 1.7 L'Annexe 4 comprend les Clauses Contractuelles Type de l'Union Européenne qui s'appliquent en cas de transfert de Données à Caractère Personnel par le Responsable de Traitement vers un pays en dehors de l'Espace Economique Européen, comme décrit plus en détail au paragraphe 2.3 ci-dessous.
- 1.8 Les Parties mettront les annexes à jour pendant la durée d'application des présentes Conditions de Traitement de Données, le cas échéant.

**2. TRAITEMENT**

- 2.1 Le Sous-Traitant et le Responsable de Traitement doivent, dans les meilleurs délais, s'adresser l'un à l'autre toutes les informations nécessaires pour permettre le respect en bonne et due forme de la Législation sur la Protection des Données à Caractère Personnel. .
- 2.2 Le Traitement de Données à Caractère Personnel a lieu dans le pays / lieu ou les pays / lieux détaillés en Annexe 1. En concluant un Contrat, le Responsable de Traitement autorise expressément le Traitement de Données à Caractère Personnel dans les pays / lieux mentionnés en Annexe 1.
- 2.3 Lorsque le Traitement de Données à Caractère Personnel effectué par le Sous-Traitant aura lieu dans un pays situé en dehors de l'Espace Economique Européen (EEE) et qui n'a pas été considéré par décision de la Commission Européenne comme apportant un niveau de protection des Données à Caractère Personnel adéquat, les Parties, pour s'assurer de garanties contractuelles appropriées de protection, les parties se conformeront à leurs obligations respectives selon les Clauses Contractuelles Types de l'Union Européenne jointes en Annexe 4 aux présentes Conditions de Traitement de Données (ou toute autre mesure de protection appropriée que l'Autorité de Protection des Données ou un législateur compétent décide comme étant de niveau suffisant pour une protection de Données à Caractère Personnel) et le Responsable de Traitement consent par la présente et donne instruction au Sous-Traitant de mener à bien ce Traitement.

**3. RESPONSABILITES DU SOUS-TRAITANT**

- 3.1 Le Sous-Traitant Traitera les Données à Caractère Personnel en bonne et due forme et avec diligence conformément aux présentes Conditions de Traitement des Données et s'assurera de se conformer à la Législation sur la Protection des Données à Caractère Personnel.
- 3.2 Le Sous-Traitant Traitera les Données à Caractère Personnel exclusivement conformément à l'exécution du Contrat et en application des instructions écrites remises par le Responsable de Traitement, sauf si le Sous-Traitant est légalement tenu de Traiter les Données à Caractère Personnel d'une manière qui y serait contraire. Dans ce dernier cas, le Sous-Traitant informera le Responsable de Traitement des dispositions légales pertinentes et de ses obligations y afférentes.
- 3.3 Le Sous-Traitant Traitera uniquement les Données à Caractère Personnel selon les finalités pour lesquelles il a reçu des instructions et pour remplir les obligations qui lui ont été confiées selon les présentes Conditions de Traitement de Données. Le Sous-Traitement n'utilisera pas les Données à Caractère Personnel à d'autres fins.
- 3.4 Le Sous-Traitant ne fournira pas les Données à Caractère Personnel à un tiers (autre que la Personne Concernée ou les autres personnes agréées par le Responsable de Traitement ou le Sous-Traitant pour procéder au Traitement des Données à Caractère Personnel), à moins que cet échange n'ait lieu en suivant les instructions du Responsable de Traitement ou dans le cadre de l'exécution des présentes Conditions de Traitement de Données (y compris ses annexes) ou lorsque cela est nécessaire pour se conformer à une obligation légale.
- 3.5 Le Sous-Traitant s'interdit d'altérer, de modifier, éditer ou changer de quelque manière que ce soit les Données à Caractère Personnel sans instruction émanant du Responsable de Traitement de le faire.
- 3.6 Le Sous-Traitant coopérera de manière raisonnable avec le Responsable de Traitement pour répondre aux demandes de la Personne Concernée en ce qui concerne l'exercice de ses droits conformément à la Législation sur la Protection des Données à Caractère Personnel, telles que, sans limitation (i) octroyer l'accès de la Personne Concernée à ses Données à Caractère Personnel; (ii) rectifier ou effacer les Données à Caractère Personnel à la demande de la Personne Concernée; (iii) apporter la preuve de la rectification ou de l'effacement de ses Données à Caractère Personnel; (iv) fournir les Données à Caractère Personnel, que la Personne Concernée a fournies au Responsable de Traitement et que le Responsable de Traitement a transmises au Sous-Traitant et ; (v) transmettre toutes Données à Caractère Personnel de la Personne Concernée à un autre Responsable de Traitement (portabilité des données). Si la demande consiste en la restitution ou en la fourniture d'une copie des Données à Caractère Personnel, le Sous-Traitant fournira les Données à Caractère Personnel sous un format structuré, couramment utilisé et lisible par machine.
- 3.7 Dans l'hypothèse où le Sous-Traitant reçoit une demande ou une objection d'une Personne Concernée (qui pourrait être une demande (sans limitation) d'information, d'accès, de rectification, de transfert de données, de limitation de traitement ou le transfert de Données à Caractère Personnel), le Sous-Traitant transmettra immédiatement cette demande au Responsable de Traitement.
- 3.8 Le Sous-Traitant conservera un registre avec toutes les catégories d'activités de Traitement effectuées pour le compte du Responsable de Traitement, conformément à la Législation sur la Protection des Données à Caractère Personnel. Le Sous-Traitant fournira au Responsable de Traitement toutes les informations nécessaires dans ce même cadre.
- 3.9 Le Sous-Traitant devra assister le Responsable de Traitement, si cela concerne des technologies ou procédures du Sous-Traitant, lorsqu'une Analyse d'Impact de Protection des Données est requise par la Législation sur la Protection des Données à Caractère Personnel.
- 3.10 Si le Responsable de Traitement fait l'objet d'une demande spécifique d'information émanant de la Personne Concernée ou d'un tiers autorisé à émettre de telles demandes (autre que la Personne Concernée ou les autres personnes agréées par le Responsable de Traitement ou le Sous-Traitant afin de procéder au Traitement de Données à Caractère Personnel), le Sous-Traitant assistera le Responsable de Traitement dans ce cadre. Le Sous-Traitant ne devra pas prendre d'action en ce qui concerne une demande reçue de la Personne Concernée ou d'un tiers (autre que la Personne Concernée ou les autres personnes agréées par le Responsable de Traitement ou le Sous-Traitant afin de procéder au Traitement de Données à Caractère Personnel), sauf si c'est en application de toute instruction préalable du Responsable de Traitement. Si une Personne Concernée contacte le Sous-Traitant pour

faire valoir ses droits conformément à la Législation sur la Protection des Données à Caractère Personnel, le Sous-Traitant devra transmettre cette demande immédiatement au Responsable de Traitement.

#### 4 RESPONSABILITES DU RESPONSABLE DE TRAITEMENT

- 4.1 Le Responsable de Traitement est responsable du caractère licite du Traitement des Données à Caractère Personnel et de la conformité à la Législation sur la Protection des Données à Caractère Personnel, y compris sans limitation à la protection des droits des Personnes Concernées.
- 4.2 Il appartient exclusivement au Responsable de Traitement de déterminer les finalités pour lesquelles et les moyens avec lesquels les Données à Caractère Personnel devront faire l'objet d'un Traitement.
- 4.3 Le Responsable de Traitement est responsable d'informer les Personnes Concernées et de garantir les droits dont les Personnes Concernées peuvent se prévaloir en application de la Législation sur la Protection des Données à Caractère Personnel et autres lois et réglementations applicables en matière de vie privée et de communiquer avec les Personnes Concernées.
- 4.4 Le Responsable de Traitement garantit que les Données à Caractère Personnel collectées sont adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles les Données à Caractère Personnel ont été transférées et (ensuite) Traitées.
- 4.5 Le Responsable de Traitement informera immédiatement le Sous-Traitant, si le Traitement est entaché d'erreurs ou d'irrégularités.
- 4.6 Le Responsable de Traitement devra mettre à disposition toute information dont le Sous-Traitant pourra avoir besoin pour le Traitement, dans les délais appropriés et au format convenu tel que précisé en Annexe 1.
- 4.7 Le Responsable de Traitement aura la charge et assumera la responsabilité de (que ce soit entre les parties elles-mêmes ou envers les Personnes Concernées et l'Autorité de Protection des Données): (i) s'assurer que les Personnes Concernées ont donné leur consentement de manière appropriée pour le Traitement de toute Donnée Personnelle par le Sous-Traitant (ou tout Sous-Traitants Ultérieurs) et/ou s'assurer qu'ils disposent de la base juridique pour le faire ; et (ii) de toute réclamation ou action en justice découlant des actions du Sous-Traitant dans la mesure où ces actions résultent d'instructions reçues par le Responsable de Traitement.

#### 5 SOUS TRAITANTS ULTERIEURS

- 5.1 Le Sous-Traitant n'engagera pas de Sous-Traitants Ultérieurs sans l'approbation préalable du Responsable de Traitement. En concluant le Contrat, le Responsable de Traitement autorise le Sous-Traitant de sous-traiter aux Sous-Traitants Ultérieurs listés en Annexe 3 ou dans un Bon de Commande.
- 5.2 Le Sous-Traitant informera le Responsable de Traitement par écrit de toutes modifications envisagées, par exemple concernant le remplacement d'un Sous-Traitant Ulérieur. Le Responsable de Traitement pourra s'opposer à ces modifications par écrit, dans les 7 jours suivant la notification écrite d'une telle modification, adressée aux Sous-Traitants Ultérieurs.
- 5.3 Le recours à un Sous-Traitant Ulérieur n'affecte aucunement les obligations du Sous-Traitant envers le Responsable de Traitement. L'accès aux Données à Caractère Personnel pertinentes ne pourra être octroyé au Sous-Traitant Ulérieur qu'à partir du moment où le Sous-Traitant Ulérieur se sera conformé (ou garantit se conformer) à tous égards aux obligations prévues aux présentes Conditions de Traitement de Données à Caractère Personnel. Le Sous-Traitant signera un accord écrit avec les Sous-Traitants Ultérieurs en ce qui concerne la sous-traitance de Donnée à caractère Personnel, qui sera conforme avec la Législation sur les Données à Caractère Personnel, et, dans la mesure du possible, contenant substantiellement les mêmes termes que les présentes Conditions de Traitement de Données à Caractère Personnel.
- 5.4 L'Annexe 3 liste les Sous-Traitants Ultérieurs actuels, les lieux de Traitement et la description des services. Les Parties mettront cette Annexe à jour, si nécessaire et dans un délai raisonnable après une modification, pendant la durée du Contrat.
- 5.5 Lorsque le Sous-Traitant sous-traite l'une ou plusieurs de ses obligations à un Sous-Traitant Ulérieur agréé par le Responsable de Traitement (par le biais du Contrat ou si en dehors du Contrat par approbation postérieure), le Sous-Traitant reste tenu de l'exécution des présentes Conditions de Traitement de Données à Caractère Personnel par les actes de ces Sous-Traitants Ultérieurs.
- 5.6 Lorsque le Sous-Traitant sous-traite l'une ou plusieurs de ses obligations à un Sous-Traitant Ulérieur, le Responsable de Traitement peut (dans certaines circonstances) fournir des instructions directement aux Sous-Traitants Ultérieurs concernant le Traitement de ses Données à Caractère Personnel par le Sous-Traitant Ulérieur. Dans un tel cas, le Sous-Traitant ne sera pas tenu responsable des manquements aux présentes Conditions de Traitement de Données à Caractère Personnel qui résulteraient des actes commis par le Sous-Traitant Ulérieur sur instructions du Responsable de Traitement, que le Sous-Traitant en soit ou non informé.

#### 6 VIOLATIONS DE SECURITE ET DE DONNEES

- 6.1 Le Sous-Traitant prendra les mesures de sécurité techniques et opérationnelles qui respectent la Législation sur la Protection des Données à Caractère Personnel et adoptera les bonnes pratiques du secteur d'activité nécessaires pour garantir la disponibilité, l'intégrité et la confidentialité des Données à Caractère Personnel et de les protéger contre toute perte ou tout Traitement illicite. Afin d'assurer le respect de la présente clause, le Responsable de Traitement informera le Sous-Traitant de tous critères de fiabilité qui s'appliquent au Traitement et fournira toute l'information nécessaire suffisamment en avance en cas de demande de modification des critères de fiabilité du Traitement de Données à Caractère Personnel.
- 6.2 Les mesures de sécurité techniques et opérationnelles seront décrites en Annexe 2 des présentes et seront conformes aux normes de sécurité généralement admises. Le Responsable de Traitement reconnaît qu'il estime que les mécanismes décrits en Annexe 2 seront suffisants pour garantir la sécurité appropriée des Données à Caractère Personnel conformément à la Législation sur la Protection des Données à Caractère Personnel.
- 6.3 Le Sous-Traitant notifiera au Responsable de Traitement toute Violation de Données dans les meilleurs délais après en avoir pris connaissance.
- 6.4 La notification mentionnée à l'article 6.3 ci-dessus indiquera à tout le moins :
- La nature de la Violation de Données, y compris, si possible, les catégories et le nombre approximatif de Personnes Concernées et les catégories et le nombre approximatifs d'enregistrements de Données à Caractère Personnel concernés ;
  - Le nom et les coordonnées du Délégué à la Protection des Données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
  - Les conséquences probables de la Violation de Données ;
  - Les mesures prises ou que le Sous-Traitant propose de prendre pour remédier à la Violation de Données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
- 6.5 Le Sous-Traitant aidera le Responsable de Traitement à remplir ses obligations légales d'information envers toutes autorités de contrôle et/ou les Personnes Concernées, en cas de Violation de Données.
- 6.6 Au cas où le Sous-Traitant estime que les instructions de Traitement données par le Responsable de Traitement ne sont pas conformes à une Législation sur la Protection des Données à Caractère Personnel, il en informera le Responsable de Traitement immédiatement.

#### 7 CLAUSES SUPPLEMENTAIRES DE CONFIDENTIALITE

7.1 Le Sous-Traitant préservera la confidentialité des Données à Caractère Personnel qu'il traite en application du Contrat et prendra toutes les mesures nécessaires pour garantir la confidentialité des Données à Caractère Personnel. Le Sous-Traitant imposera aussi le devoir de confidentialité à son personnel et à toute personne qu'il aura engagée, et qui ont accès aux Données à Caractère Personnel.

7.2 Le devoir de confidentialité indiqué au présent Article ne s'applique pas dès lors que le Responsable de Traitement a donné sa permission écrite de fournir les Données à Caractère Personnel à un tiers ou qu'il existe une obligation légale de fournir celles-ci à un Tiers.

## 8 AUDITS DE PROTECTION DES DONNEES

8.1 Le Sous-Traitant autorise le Responsable de Traitement à vérifier si le Sous-Traitant respecte les présentes Conditions de Traitement de Données ou bien un audit par l'intermédiaire d'auditeurs indépendants, aux frais du Responsable de Traitement, sans utiliser d'informations confidentielles du Sous-Traitant et sans perturber les activités opérationnelles du Sous-Traitant. Si l'audit indique que le Sous-Traitant ne respecte pas ses obligations en application des présentes Conditions de Traitement de Données à Caractère Personnel, le Sous-Traitant remédiera aux manquements qui auront été identifiés ou les rectifiera dans la mesure du raisonnable aussi rapidement que possible. Dans ce cas, le Sous-Traitant prendra à sa charge les coûts raisonnables et justifiés de l'auditeur (auquel cas, un paiement sera uniquement effectué sur présentation d'une facture valable des auditeurs pour lesdits coûts).

8.2 Un audit ne peut avoir lieu au maximum une fois par an, sauf si des preuves suffisantes indiquent que le Sous-Traitant ne respecte pas ses obligations au titre des présentes Conditions de Traitement de Données. Le Sous-Traitant remettra toutes les informations raisonnablement nécessaires au Responsable de Traitement pour mener l'audit.

8.3 En cas d'enquête d'une Autorité de Protection des Données ou d'une autre autorité compétente (l'« Autorité »), le Sous-Traitant fournira toute la coopération raisonnable et informera le Responsable du Traitement le plus rapidement possible.

8.4 Le Sous-Traitant désignera une personne physique comme point de contact du Responsable de Traitement pour l'aider à remplir ses obligations de communication découlant du Traitement et le Sous-Traitant indiquera les coordonnées du point de contact au Responsable de Traitement.

## 9 MODIFICATIONS

9.1 Dans le cas où des amendements apportés à l'exécution d'une ou des obligations prévues au Contrat ont des conséquences sur le Traitement de Données à Caractère Personnel, le Sous-Traitant fournira au Responsable de Traitement une notification de ses propositions d'amendement des présentes Conditions de Traitement de Données par écrit (ceci peut avoir lieu par voie d'un courrier électronique). Le Responsable de Traitement fournira ses objections aux clauses modifiées dans les 10 jours ouvrables de la réception de la notification et s'il n'a pas émis d'objection, le Responsable de Traitement sera considéré comme ayant accepté les modifications.

9.2 Les avenants aux annexes des présentes Conditions de Traitement de Données à Caractère Personnel pourront avoir lieu par notification par le Sous-Traitant par écrit au Responsable de Traitement (ce qui peut avoir lieu par voie d'un courrier électronique), indiquant le numéro de version et la date d'entrée en vigueur de la nouvelle version. Les modifications substantielles des annexes ne pourront pas être faites sans avoir donné l'opportunité au Responsable de Traitement de s'y opposer.

## 10 INDEMNISATION MUTUELLE

10.1 Le Sous-Traitant indemnifiera le Responsable du Traitement et le tiendra indemne de toutes les amendes et/ou sanctions imposées au Responsable de Traitement par l'Autorité ou pour le compte de celle-ci et pour les réclamations ayant trait à toute perte et tout préjudice subi par une Personne Concernée, lorsqu'il est établi que ces amendes et/ou sanctions ou réclamations sont directement attribuables à un manquement du Sous-Traitant dans le cadre du Traitement de Données à Caractère Personnel conformément à la Législation sur la Protection des Données ou toute autre législation applicable en matière de vie privée.

Pour pouvoir se prévaloir du présent paragraphe 10.1, le Responsable de Traitement sera tenu:

- (i) de notifier immédiatement par écrit au Sous-Traitant l'existence et l'objet de la réclamation d'une Personne Concernée ou toute enquête ou autre instruction qui pourrait conduire l'Autorité de protection des Données à envisager ou décider d'imposer une sanction ou de demander l'imposition d'une sanction ;
- (ii) d'agir et de communiquer avec l'Autorité de Protection des Données ou la Personne Concernée en consultation avec le Sous-Traitant;
- (iii) de s'opposer aux amendes imposées ou d'interjeter appel contre celles-ci s'il existe une raison de le faire ; et
- (iv) de laisser le contrôle du dossier, y compris le fait de procéder à d'éventuels règlements amiables, entièrement au Sous-Traitant. A cette fin, le Responsable de Traitement accordera les procurations et la coopération nécessaires au Sous-Traitant et lui remettra les informations nécessaires pour se défendre contre ces actions en justice, si nécessaire au nom du Responsable de Traitement.

10.2 Le Responsable de Traitement indemnifiera le Sous-Traitant et le dégagera de toute responsabilité pour les amendes et/ou les sanctions imposées au Sous-Traitant par ou pour le compte de l'Autorité de Protection des Données et pour les réclamations en cas de perte ou de préjudices subis par une Personne Concernée, lorsqu'il est établi que ces sanctions et/ou sanctions pécuniaires ou réclamations sont attribuables à un non-respect de la part du Responsable de Traitement de la Législation sur la Protection des Données à Caractère Personnel ou d'une autre législation applicable en matière de vie privée.

Pour se prévaloir du présent paragraphe 10.2, le Sous-Traitant sera tenu:

- (i) De notifier par écrit sans tarder au Responsable de Traitement l'existence et l'objet de la réclamation d'une Personne Concernée ou toute enquête ou autre instruction qui pourrait conduire l'Autorité de Protection des Données à envisager ou décider d'imposer une sanction ou de demander l'imposition d'une sanction ;
- (ii) D'agir et de communiquer avec l'Autorité de Protection des Données ou avec la Personne Concernée en consultation avec le Responsable de Traitement ;
- (iii) De s'opposer aux amendes imposées ou d'interjeter appel contre celles-ci s'il existe une raison de le faire ; et
- (iv) de laisser le contrôle du dossier, y compris le fait de procéder à un règlement amiable, entièrement au Responsable de Traitement. A cette fin, le Sous-Traitant accordera les procurations et la coopération nécessaires au Responsable de Traitement et lui remettra les informations nécessaires pour se défendre contre ces actions en justice, si nécessaire au nom du Sous-Traitant.

10.3 Dans la mesure où les Parties se partagent la responsabilité (de manière solidaire ou conjointe ou autrement) envers les Tiers, y compris la (les) Personne(s) Concernée(s), ou se voient imposer une amende conjointe par l'Autorité de Protection des Données, les Parties resteront tenues de s'indemniser mutuellement selon les paragraphes 10.1 et 10.2 de la partie de l'amende proportionnelle à leur part de responsabilité pour le fait générateur de cette responsabilité ou de cette amende conjointe, en tenant compte de la décision de toute juridiction ou tribunal compétent, l'Autorité de Protection des Données et la contribution prise dans la violation par une Partie de ses obligations selon les présentes Conditions de Traitement de Données.

## 11 DUREE ET RESILIATION

- 11.1 Les présentes Conditions de Traitement de Données entrent en vigueur à la date du Contrat.
- 11.2 Lors de la résiliation du Contrat, le Sous-Traitant devra restituer – ou à la demande du Responsable de Traitement détruire ou conserver – les Données à Caractère Personnel de la manière définie en Annexe 1. Dans le cas où les Données à Caractère Personnel sont détenues ou conservées dans un système informatique ou sous toute autre forme qui empêche toute transmission raisonnable au Responsable de Traitement, le Sous-Traitant détruira immédiatement les Données à Caractère Personnel sur ses systèmes, sauf accord contraire des Parties.

**Annexes:**

**Annexe 1:** Description du Traitement de Données à Caractère Personnel

**Annexe 2:** Mesures de Sécurité

**Annexe 3:** Sous-Traitants Ultérieurs

**Annexe 4:** Clause Contractuelle Type de l'Union Européenne

## ANNEXE 1 - DESCRIPTION DU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

### 1. LES DONNÉES A CARACTERE PERSONNEL QUI SERONT TRAITEES:

Produit	Les Données à Caractère Personnel susceptibles de faire l'objet d'un traitement pourraient inclure:	Données à Caractère Personnel de qui:
Unit4 ERP 7	Noms ; adresses ; détails du contrat ; numéros de téléphone (y compris de portable) ; adresse(s) électronique(s) ; autres coordonnées ; date de naissance ; âge ; lieu de naissance ; nationalité ou citoyenneté ; résidence ; domicile ; langue(s) parlée(s) ; numéro de passeport ; numéro de sécurité nationale ou numéro de sécurité sociale ou référence de carte d'identité ; état civil ; détails du bénéficiaire des prestations ; sexe ; informations sur l'emploi (y compris : salaire ; poste ; échelle de rémunération ; échelon de rémunération ; compétences et notes personnelles) ; informations fiscales ; informations sur les prestations ; appartenance à un syndicat ; proches parents fournis (nom ; adresse ; date de naissance ; numéro de téléphone ; coordonnées en cas d'urgence) ; dates de début et de fin d'emploi ; coordonnées du compte bancaire ou de la carte de crédit ; coordonnées de la société de services à la personne (nom ; numéro d'enregistrement et siège social) ; mandats d'administrateur ; numéros de TVA ; documents (écrits ou électroniques) contenant l'un des éléments ci-dessus.	Anciens membres du personnel et membres actuels ;  Prestataires ou sous-traitants (de quelque type que ce soit), mandataires ou administrateurs ; et Candidats à l'embauche ou salariés potentiels.
Unit4 Financials	Noms ; adresses ; informations contractuelles ; numéros de téléphone (y compris téléphone portable) ; adresse(s) électronique(s) ; autres coordonnées, date de naissance, âge, lieu de naissance, nationalité ou citoyenneté ; lieu de résidence, domicile, langue(s) parlée(s) ; numéro de passeport ; numéro de sécurité sociale ou numéro de sécurité nationale ou référence de carte d'identité ; état civil ; coordonnées des bénéficiaires d'avantages ; sexe ; information sur l'emploi (y compris : salaire, poste ; échelle salariale, échelon salarial ; compétences et notes personnelles) ; données fiscales ; données sur les avantages perçus ; appartenance à un syndicat ; proche parent (nom, adresse, date de naissance, numéro de téléphone, coordonnées d'une personne à contacter en cas d'urgence), date d'embauche et date de rupture d'emploi ; coordonnées du compte bancaire ou de carte de crédit ; coordonnées des entreprises de services unipersonnelles (nom ; numéro d'immatriculation et siège social) ; mandats sociaux ou postes de direction ; numéros de TVA ; documents (écrits ou électroniques) contenant l'un des éléments précités.	Anciens membres du personnel et membres actuels ;  Prestataires ou sous-traitants (de quelque type que ce soit), mandataires ou administrateurs ; et Candidats à l'embauche ou salariés potentiels.
Unit4 Student Management	Noms ; adresses ; informations contractuelles ; numéros de téléphone (y compris le portable) ; adresse(s) électronique(s) ; autres coordonnées ; date de naissance ; âge ; lieu de naissance ; nationalité ou citoyenneté ; résidence ; domicile ; langue(s) parlée(s) ; numéro de passeport ; numéro de sécurité nationale ou numéro de sécurité sociale ou référence de carte d'identité ; état civil ; coordonnées des bénéficiaires recevant des avantages ; sexe ; information sur l'emploi (y compris : salaire ; poste ; échelle salariale, échelon salarial ; compétences et notes personnelles) ; données fiscales ; données sur les avantages ; appartenance syndicale ; proche parent (nom ; adresse ; date de naissance ; numéro de téléphone ; coordonnées d'une personne à contacter en cas d'urgence) ; dates d'embauche et de rupture d'emploi ; coordonnées bancaires ou de carte de crédit ; coordonnées des entreprises de services unipersonnelles (nom ; numéro d'immatriculation et siège social) ; mandats sociaux ou postes de direction ; numéros de TVA ; documents (écrits ou électroniques) contenant l'un quelconque des éléments précités.  Données à Caractère Personnel supplémentaires pour les anciens salariés et salariés actuels : type de personnel (p. ex. faculté, conseiller, directeur du logement) ; département universitaire ; statut à l'embauche ; statut d'emploi ; charge de travail ; rang occupé au sein du corps professoral ; publications ; suivi du statut professionnel ; données sur le parcours académique et informations sur les qualifications.  Données à Caractère Personnel supplémentaires pour les anciens candidats et candidats actuels : information sur l'université précédente, relevés des notes scolaires et/ou résultats de tests (supplémentaires) ; état de santé physique ; lettres d'anciens employeurs et information sur les lieux de travail.  Données à Caractère Personnel supplémentaires pour les anciens étudiants et étudiants actuels : dossier scolaire y compris les résultats et objectifs ; données sur l'inscription ; données sur la progression académique (y compris les notes obtenues) ; résultats scolaires ; stages professionnels ou universitaires ; données sur la planification des cours ; historique des factures et paiements ; préférences et historique de logement ; données sur l'aide financière ; dossier de santé (y compris les vaccins, les allergies et l'état de santé) ; information sur l'assurance et documentation sur la santé.	Anciens membres du personnel et membres du personnel actuels (y compris le corps professoral et les autres membres du personnel) ; Les prestataires ou sous-traitants (de quelque type que ce soit), mandataires ou administrateurs ; Les candidats à l'embauche ou salariés potentiels ; et Les anciens étudiants ainsi que les étudiants actuels et potentiels
Unit4 FP&A	Noms ; adresses ; numéros de téléphone (y compris de portable) ; adresse(s) électronique(s) ; autres coordonnées. Il n'est pas nécessaire de stocker ou de traiter d'autres données personnelles pour atteindre les objectifs du produit (tels que définis ci-dessous), mais d'autres données personnelles peuvent être stockées ou traitées par le produit si elles sont configurées de manière à le faire (par exemple, des données sur les salaires) ou sont saisies dans le produit par le client.	Anciens membres du personnel et membres du personnel actuels ; Sous-traitants (de quelque type que ce soit), mandataires ou administrateurs
Unit4 Assistance PSA Suite	Noms ; adresses ; numéros de téléphone (y compris portable) ; adresse(s) électronique(s) ; autres coordonnées. Il n'est <u>pas nécessaire</u> d'avoir d'autre Donnée Personnelle à conserver ou à traiter pour atteindre les finalités du Produit -tel qu'indiqué ci-dessous) ; cependant d'autres Données à Caractère Personnel peuvent être conservées ou traitées par le Produit s'il est configuré pour le faire ou si des Données à Caractère Personnel sont ajoutées par le Client sur le Produit.	Anciens membres du personnel et membres actuels du personnel ; Sous-traitants (de quelque forme que ce soit), mandataires ou administrateurs. Toute autre personne faisant partie d'une équipe projet (y compris des personnes ne faisant pas partie du personnel) candidats à l'embauche ou salariés potentiels

		Clients et fournisseurs du Client
Unit4 Talent Management	<p>Noms; adresses; coordonnées; numéros de téléphone (y compris portable); adresse(s) électronique(s); autres coordonnées (adresse, nom de la rue et pays), date de naissance; âge; lieu de naissance; poste; département.</p> <p>En utilisant le module « Learn » : inscriptions à des cours; inscriptions à des sessions; résultats de tests et appréciations; données vidéos, textes et présentations d'implication; badges; certificats.</p> <p>En utilisant le module « Perform » : données d'enregistrement, données relatives aux objectifs et résultats clés (OKR), retours et évaluations.</p> <p>En utilisant le module « Engage » : réponses et retours sur les questions d'implication de l'employé.</p>	<p>Anciens membres du personnel et membres actuels</p> <p>Anciens candidats à l'embauche et candidats actuels;</p> <p>Prestataires ou sous-traitants (de quelque forme que ce soit) agents ou dirigeants; et</p> <p>Candidats à l'embauche ou salariés potentiels.</p>
People Platform Services ("PPS") (généralement) comprenant IDS et Wanda (comprenant tout service associé	<p>Etant donné que les PPS fonctionnent et s'interface avec d'autres Produits et Services Unit4, il peut y avoir des traitements de tous les types de Données à Caractère Personnel décrites dans le présent tableau en ce qui concerne les Produits et les Services qui y sont identifiés.</p> <p>En outre: Wanda peut traiter : les identifiants Unit4Id (qui identifient l'utilisateur d'IDS), toute Donnée à Caractère Personnel ou information fournie par l'utilisateur sur une application à laquelle Wanda est connectée (ladite information étant traitée ou conservée sauf si l'utilisateur choisit de la faire supprimer); toute donnée de conversation et dialogue, métadonnée susceptible d'être attribuée à une personne physique ainsi que les Application Insights Logs (un service Microsoft utilisé afin d'établir des diagnostics).</p>	<p>Toutes les personnes physiques listées dans le présent tableau.</p> <p>En fonction de l'application à laquelle ou du service auquel Wanda est connecté, le PPS est susceptible de Traiter des Données à Caractère Personnel relative à toute personne physique vivante que l'Utilisateur choisit d'indiquer.</p>

## 2. NATURE ET FINALITES DU TRAITEMENT:

En règle générale, la nature du Traitement effectué par le Sous-Traitant ne sera que ce qui est nécessaire pour que le Sous-Traitant puisse remplir ses obligations et exercer ses droits au titre du Contrat y compris (en ce qui concerne les Données à Caractère Personnel) 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. L'objet ou la finalité du Traitement consiste pour le Sous-Traitant à exécuter ses obligations et l'exercice de ses droits conformément aux présentes Conditions de Traitement de Données, y compris l'exécution de fonctions demandées ou requises par le Responsable de Traitement pour le respect par ce dernier de ses obligations légales et/ou contractuelles. Dans le cadre et en fonction du Produit ou le Service, le Traitement comprendra ce qui suit :

Produit	Nature et finalité du traitement
Unit4 ERP 7	<p>Les Données à Caractère Personnel seront saisies dans Unit4 ERP 7, ce qui permettra au Client d'organiser et de gérer les processus liés au fonctionnement opérationnel ainsi que les processus de gestion et/ou d'administration de ses activités internes. Ces processus incluent notamment :</p> <ul style="list-style-type: none"> <li>• les demandes de déplacements ;</li> <li>• le traitement des demandes de remboursement de frais ;</li> <li>• le traitement des feuilles de précense ;</li> <li>• la gestion des absences</li> <li>• les processus liés aux RH et à l'administration de la paie : <ul style="list-style-type: none"> <li>• l'administration de la paie ;</li> <li>• l'inscription à des cursus ;</li> <li>• la gestion des compétences ;</li> <li>• les évaluations ;</li> <li>• l'examen des salaires ;</li> <li>• inscription des candidats à l'embauche ;</li> <li>• le traitement des paiements</li> <li>• facturation</li> <li>• demandes d'achats</li> <li>• la planification des ressources humaines/projets</li> </ul> </li> </ul> <p>Le Traitement impliquera :</p> <p><b>Produit (solution logicielle)</b></p> <p>Exécution par Unit4 ERP 7 de codes logiciels programmables nécessaires au déroulement des activités énoncées (ci-dessus). Il peut s'agir d'un transfert de données vers ou depuis des solutions de Tiers échappant au contrôle du Sous-Traitant via des intégrations.</p> <p><b>Services</b></p>

	<p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des services supplémentaires Unit4 Cloud, comme indiqué en détails dans la Description des Services Unit4 Cloud ou dans les Services People Platform (tels que décrits dans la Description de Service People Platform applicable) ;</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 ERP 7 et assistance du client dans l'exploitation de la solution, comme décrit en détail dans les Conditions d'Assistance Unit4.</p> <p>Accès aux Données à Caractère Personnel pour offrir une configuration et/ou une personnalisation et/ou une migration de données (par exemple depuis ses anciens systèmes) et/ou d'autres Services professionnels achetés par le Client.</p>
Unit4 Financials	<p>Les Données à Caractère Personnel seront saisies dans Unit4 Financials, ce qui permettra au Client d'organiser et de gérer les processus liés au fonctionnement opérationnel ainsi que les processus de gestion et/ou d'administration de ses activités internes. Ces processus incluent notamment :</p> <ul style="list-style-type: none"> <li>• l'inscription d'un client/fournisseur/salarié ;</li> <li>• le traitement des paiements ;</li> <li>• la facturation ;</li> <li>• le traitement des demandes de remboursement de frais ;</li> <li>• les demandes de déplacements ;</li> <li>• les demandes d'achat et les commandes ;</li> <li>• la planification des ressources humaines/projets ;</li> <li>• les processus liés aux RH et à l'administration de la paie : <ul style="list-style-type: none"> <li>• l'administration de la paie ;</li> <li>• le traitement des feuilles de présence ;</li> <li>• la gestion des absences ;</li> <li>• l'inscription à des cursus ;</li> <li>• la gestion des compétences ;</li> <li>• les évaluations ;</li> <li>• l'examen des salaires ;</li> <li>• inscription des candidats à l'embauche ;</li> </ul> </li> </ul> <p>Le Traitement impliquera :</p> <p><b>Produit (solution logicielle)</b></p> <p>Exécution par Unit4 Financials de codes logiciels programmables nécessaires au déroulement des activités énoncées (ci-dessus). Il peut s'agir d'un transfert de données vers ou depuis des solutions de Tiers échappant au contrôle du Sous-Traitant via des intégrations.</p> <p><b>Services</b></p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des services supplémentaires Unit4 Cloud, comme indiqué en détails dans la Description des Services Unit4 Cloud ou dans les Services People Platform (tels que décrits dans la Description de Service People Platform applicable) ;</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 Financials et assistance du client dans l'exploitation de la solution, comme décrit en détail dans les Conditions d'Assistance Unit4.</p> <p>Accès aux Données à Caractère Personnel pour offrir une configuration et/ou une personnalisation et/ou une migration de données (par exemple depuis ses anciens systèmes) et/ou d'autres Services professionnels achetés par le Client.</p>
Unit4 Student Management	<p>Les Données à Caractère Personnel seront saisies dans Unit4 Student Management, ce qui permettra au Client d'organiser et de gérer les processus liés au fonctionnement opérationnel ainsi que les processus de gestion et/ou d'administration de ses activités internes. Ces processus incluent notamment :</p> <ul style="list-style-type: none"> <li>• le recrutement d'étudiants potentiels ;</li> <li>• la réponse à des demandes de renseignements ;</li> <li>• les demandes de traitement ;</li> <li>• la gestion du cycle de vie universitaire d'un étudiant, y compris l'inscription, la planification des cours, la progression académique, les conseils, le logement et d'autres services, l'obtention du diplôme ;</li> <li>• la planification et l'établissement des horaires pour le personnel de l'université.</li> </ul> <p>Le Traitement impliquera :</p> <p><b>Produit (solution logicielle)</b></p> <p>Exécution par Unit4 Student Management de codes logiciels programmables nécessaires au déroulement des activités énoncées ci-dessus. Il peut s'agir d'un transfert de données vers ou depuis des solutions de Tiers échappant au contrôle du Sous-Traitant via des intégrations.</p> <p><b>Services</b></p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des services supplémentaires Unit4 Cloud, comme indiqué en détails dans la Description des Services Unit4 Cloud ou des Services People Platform (tels que détaillés dans la Description de Service People Platform applicable).</p>

	<p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 Student Management et assistance du client dans l'exploitation de la solution, comme décrit en détail dans les Conditions d'Assistance Unit4.</p> <p>Accès aux Données à Caractère Personnel pour offrir une configuration et/ou une personnalisation et/ou une migration de données (par exemple depuis les anciens systèmes) et/ou d'autres Services professionnels achetés par le Client.</p>
Unit4 FP&A	<p>Les Données à Caractère Personnel seront saisies dans Unit4 FP&amp;A, ce qui permettra au Client d'organiser et de gérer les processus liés au fonctionnement opérationnel ainsi que les processus de gestion et/ou d'administration de ses activités internes. Ces processus incluent notamment :</p> <ul style="list-style-type: none"> <li>• Budgétisation ;</li> <li>• Rapports financiers et autres ;</li> <li>• Distribution des rapports ;</li> <li>• Traitement des approbations ;</li> <li>• Planification des ressources humaines/projets.</li> </ul> <p>Le traitement impliquera :</p> <p><b>Produit (solution logicielle)</b></p> <p>Exécution par Unit4 FP&amp;A de codes logiciels programmables nécessaires au déroulement des activités énoncées (ci-dessus). Il peut s'agir d'un transfert de données vers ou depuis des solutions de Tiers échappant au contrôle du Sous-Traitant via des intégrations.</p> <p><b>Services</b></p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des services supplémentaires Unit4 Cloud, comme indiqué en détails dans la Description des Services Unit4 Cloud ou dans les Services People Platform (tels que décrits dans la Description de Service People Platform applicable) ;</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 FP&amp;A et assistance du client dans l'exploitation de la solution, comme décrit en détail dans les Conditions d'Assistance Unit4.</p> <p>Accès aux Données à Caractère Personnel pour offrir une configuration et/ou une personnalisation et/ou une migration de données (par exemple depuis ses anciens systèmes) et/ou d'autres Services professionnels achetés par le Client.</p>
Unit4 Talent Management	<p>Les Données à Caractère Personnel seront saisies dans Unit4 Talent Management, ce qui permettra au Client d'organiser et de gérer les processus liés au fonctionnement opérationnel ainsi que les processus de gestion et/ou d'administration de ses activités internes. Ces processus incluent notamment :</p> <ul style="list-style-type: none"> <li>• Gestion des ressources humaines;</li> <li>• Gestion de la performance du personnel;</li> <li>• Développement de talent;</li> <li>• Evaluation de candidat;</li> <li>• Acquisition de savoir -" Learning";</li> <li>• Retours et appreciation; et</li> <li>• Statistiques sur le personnel et l'implication du personnel</li> </ul> <p>Le traitement impliquera :</p> <p><b>Produit (solution logicielle)</b></p> <p>Exécution par Unit4 Talent Management de codes logiciels programmables nécessaires au déroulement des activités énoncées (ci-dessus). Il peut s'agir d'un transfert de données vers ou depuis des solutions de Tiers échappant au contrôle du Sous-Traitant via des intégrations.</p> <p><b>Services</b></p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des services supplémentaires Unit4 Cloud, comme indiqué en détails dans la Description des Services Unit4 Cloud ou dans les Services People Platform (tels que décrits dans la Description de Service People Platform applicable) ;</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 Talent Management et assistance du client dans l'exploitation de la solution, comme décrit en détail dans les Conditions d'Assistance Unit4.</p> <p>Accès aux Données à Caractère Personnel pour offrir une configuration et/ou une personnalisation et/ou une migration de données (par exemple depuis ses anciens systèmes) et/ou d'autres Services professionnels achetés par le Client.</p>
Unit4 Assistance PSA Suite	<p>Les Données à Caractère Personnel seront saisies sur la Suite Unit4 Assistance PSA permettant au Client d'organiser et de gérer les processus liés au fonctionnement opérationnel ainsi que les processus de gestion et/ou d'administration de ses activités internes. Ces processus incluent notamment :</p> <ul style="list-style-type: none"> <li>• Automatisation d'un département de services professionnels, y compris gestion des ressources humaines ou gestion financière ;</li> <li>• Gestion des temps d'activité quotidienne et gestion de projet</li> <li>• Saisie des temps et notes de frais avec justificatifs ;</li> <li>• Transformation d'opportunités en projets, budget et temps prévisionnels et planification de projets et de ressources</li> <li>• Suivi du temps d'activité et des notes de frais et émission de factures ;</li> <li>• Intégration de projets sur d'autres applications ;</li> <li>• Réalisation de la comptabilité par le biais d'intégration de données financières dans d'autres solutions.</li> </ul>

	<p>Le Traitement impliquera:</p> <p><b>Produit (solution logicielle)</b></p> <p>Exécution par la suite Unit4 Assistance PSA de codes logiciels programmables nécessaires au déroulement des activités énoncées ci-dessus. Il peut s'agir d'un transfert de données vers ou depuis des solutions de Tiers échappant au contrôle du Sous-Traitant via des intégrations.</p> <p><b>Services</b></p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des services supplémentaires Unit4 Cloud, comme indiqué en détails dans la Description des Services Unit4 Cloud ou des Services People Platform (tels que détaillés dans la Description de Service People Platform applicable).</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance de la Suite Unit4 Assistance PSA et assistance du client dans l'exploitation de la solution, comme décrit en détail dans les Conditions d'Assistance Unit4.</p> <p>Accès aux Données à Caractère Personnel pour offrir une configuration et/ou une personnalisation et/ou une migration de données (par exemple depuis les anciens systèmes) et/ou d'autres Services professionnels achetés par le Client.</p>
<p>People Platform Services ("PPS") (generally) including IDS and Wanda (together with any supporting services)</p>	<p>Les Données à Caractère Personnel seront saisies sur la Suite Unit4 Assistance PSA permettant au Client d'organiser et de gérer les processus liés au fonctionnement opérationnel ainsi que les processus de gestion et/ou d'administration de ses activités internes. Ces processus incluent notamment :</p> <ul style="list-style-type: none"> <li>• Automatisation d'un département de services professionnels, y compris gestion des ressources humaines ou gestion financière ;</li> <li>• Gestion des temps d'activité quotidienne et gestion de projet</li> <li>• Saisie des temps et notes de frais avec justificatifs ;</li> <li>• Transformation d'opportunités en projets, budget et temps prévisionnels et planification de projets et de ressources</li> <li>• Suivi du temps d'activité et des notes de frais et émission de factures ;</li> <li>• Intégration de projets sur d'autres applications ;</li> <li>• Réalisation de la comptabilité par le biais d'intégration de données financières dans d'autres solutions.</li> </ul> <p>Le Traitement impliquera:</p> <p><b>Produit (solution logicielle)</b></p> <p>Exécution par la suite Unit4 Assistance PSA de codes logiciels programmables nécessaires au déroulement des activités énoncées ci-dessus. Il peut s'agir d'un transfert de données vers ou depuis des solutions de Tiers échappant au contrôle du Sous-Traitant via des intégrations.</p> <p><b>Services</b></p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des services supplémentaires Unit4 Cloud, comme indiqué en détails dans la Description des Services Unit4 Cloud ou des Services People Platform (tels que détaillés dans la Description de Service People Platform applicable).</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance de la Suite Unit4 Assistance PSA et assistance du client dans l'exploitation de la solution, comme décrit en détail dans les Conditions d'Assistance Unit4.</p> <p>Accès aux Données à Caractère Personnel pour offrir une configuration et/ou une personnalisation et/ou une migration de données (par exemple depuis les anciens systèmes) et/ou d'autres Services professionnels achetés par le Client.</p>

### 3. DESCRIPTION ET MOYENS DU TRAITEMENT :

Le Sous-Traitant Traitera les Données à Caractère Personnel mentionnées ci-dessus en ce qui concerne les activités suivantes (les activités ci-dessous ne sont mentionnées qu'à titre d'exemples) :

Type de Traitement	Description	Moyens et ressources
<p>Services Cloud (SaaS Unit4 ou Managed Cloud Unit4)</p>	<p>Le Sous-Traitant Traitera les Données à Caractère Personnel en lien avec les activités décrites dans le Contrat et plus spécifiquement dans la Description de Services Cloud d'Unit4 et les descriptions de Services Spécifiques à une Solution.</p>	<p><u>Personnel</u></p> <p>L'équipe opérationnelle pour les Services Cloud d'Unit4 a des membres en Pologne, Suède, Norvège, au Royaume-Uni, aux Etats-Unis d'Amérique, au Canada, en Malaisie et à Singapour. Lesdits membres du personnel du Sous-Traitant fournissent les Services Cloud d'Unit4. .</p> <p><u>Biens et Infrastructure</u></p> <p>Unit4 utilise des services d'hébergement d'infrastructure tiers afin de fournir les Services Cloud d'Unit4 et fait appel à d'autres systèmes logiciels pour la gestion et l'exécution. Voir Annexe 3.</p>
<p>Service Cloud Gestion des Talents SaaS (Talent Management)</p>	<p>Le Sous-Traitant Traitera les Données à Caractère Personnel en lien avec les activités décrites dans le Contrat et plus spécifiquement dans la Description de Services de Gestion des Talents Cloud et</p>	<p><u>Personnel</u></p> <p>L'équipe opérationnelle Gestion des Talents Cloud d'Unit4 compte du personnel essentiellement en Belgique et autres pays de l'EEE. Lesdits membres du personnel du Sous-Traitant fournissent les Services Gestion des Talents SaaS d'Unit4.</p>

	les descriptions de Services Spécifiques à une Solution.	<p><u>Biens et Infrastructure</u></p> <p>Unit4 utilise des services d'hébergement d'infrastructure tiers pour fournir les services Gestion des Talents SaaS et utilise d'autres systèmes logiciels pour l'exploitation et la gestion. Voir Annexe 3.</p>
Support Services Services d'Assistance	Le Sous-Traitant Traitera les Données à Caractère Personnel en lien avec les activités décrites au Contrat et plus spécifiquement dans les Conditions d'Assistance Unit4 .	<p><u>Personnel</u></p> <p>L'équipe d'Assistance Unit4 compte du personnel dans ces lieux: Royaume-Uni, Pologne, Portugal, Norvège, Allemagne, Suède, Etats-Unis d'Amérique, Canada (et tout autre lieu le cas échéant si nécessaire pour les activités d'Unit4). Lesdits membres du personnel du Sous-Traitant fournissent les Services d'Assistance d'Unit4 (décrits dans les Conditions d'Assistance d'Unit4 au paragraphe B des Niveaux de Service).</p> <p><u>Biens et Infrastructure</u></p> <p>Unit4 utilise d'autres logiciels pour l'exploitation, la livraison et la gestion de ces services..</p>
Services Professionnels et/ou consultance	Le Sous-Traitant Traitera les Données à Caractère Personnel en lien avec les activités décrites au Contrat et plus spécifiquement dans toute documentation Projet plus précise ou dans les énoncés de travaux convenus entre les Parties après le début du Projet.	<p><u>Personnel</u></p> <p>L'équipe des Services Professionnels d'Unit4 compte du personnel dans tous les lieux où Unit4 a une entité y compris le Royaume Uni, l'Irlande, la Pologne, le Portugal, la Norvège, l'Espagne, la France, l'Allemagne, la Suède, les Etats-Unis d'Amérique, le Canada, Singapour / Malaisie (et tout autre lieu le cas échéant si nécessaire pour les activités d'Unit4) . Lesdits membres du personnel du Sous-Traitant fournissent les Services Professionnels Unit4.</p> <p><u>Biens et Infrastructure</u></p> <p>Unit4 utilise d'autres systèmes logiciels pour l'exploitation, la livraison et la gestion de ces services.</p>
Services Professionnels Unit4 (si sous-traités à un partenaire en charge de la livraison)	<p>Le Sous-Traitant et ses sous-traitants ultérieurs Traiteront les Données à Caractère Personnel susmentionnées en lien avec les activités décrites au Contrat et (le cas échéant) les documentations contractuelles et de service des tiers faisant partie du Contrat. Pour plus de détails, voir l'annexe 3.</p> <p>Le Sous-Traitant conclura un accord écrit avec le(s) Sous-traitants ultérieurs, qui sera conforme avec la législation et les réglementations applicables et les présentes Conditions de Traitement de Données</p> <p>En outre, en signant le Contrat, le Responsable de Traitement a autorisé au le Sous-Traitant de faire appel aux sous-traitants ultérieurs listés en Annexe 3.</p>	Voir Annexe 3.
Produits et Services Tiers	Le Sous-Traitant et ses sous-traitants ultérieurs Traiteront les Données à Caractère Personnel en lien avec les activités décrites au Contrat et dans les documentations contractuelles et de service du Fournisseur Tiers, fournies comme faisant partie du Contrat	Voir Annexe 3 et toute stipulation supplémentaire dans les annexes et appendices des présentes Conditions de Traitement de Données si cela est requis par le Fournisseur Tiers ou par el Droit Applicable.
People Platform Services ("PPS") (en règle générale) comprenant IDS et Wanda (incluant tout service d'assistance associé)	Outre les Services Cloud, les Services PPS traiteront (lorsque applicable) les Données à Caractère Personnel en lien avec une déclaration de protection de la vie privée tel que présentée à l'utilisateur final, requérant son consentement, lorsque de telles Données à Caractère Personnel sont traitées.	<p><u>Personnel</u></p> <p>L'équipe en charge des Services Cloud d'Unit4, qui exploite la plateforme PPS, compte du personnel en Pologne, Suède, Norvège, Royaume Uni, Etats-Unis d'Amérique, Canada, Malaisie et Singapour. Lesdits membres du personnel du Sous-Traitant fournissent les Services Cloud.</p> <p><u>Biens et Infrastructure</u></p> <p>Unit4 utilise ses propres services d'infrastructure et des services tiers (partagés) d'infrastructure pour fournir les services People Platform d'Unit4. Cela inclut les systèmes tiers (par exemple les applications de collaboration) sur lesquels Unit4 n'exerce aucun contrôle. Les PPS comprenant Wanda utilisent un certain nombre de produits et services Microsoft, comme suit :</p> <p>:</p> <ul style="list-style-type: none"> <li>• Cognitive services: <ul style="list-style-type: none"> <li>○ LUIS Cognitive Service - compréhension de texte.</li> <li>○ Text Translator API – traduction de texte</li> <li>○ QnA Maker Cognitive service – fournit un service de questions / réponses</li> </ul> </li> <li>• Bot framework connectors – fournit la connection de Wanda aux réseaux sociaux "supportés ».</li> </ul>

		<ul style="list-style-type: none"> <li>Traffic manager – utilisé pour la reprise d'activité après sinistre et basculement si la région principale est affectée</li> <li>Web apps / web jobs – héberge des APIs web et des processus au long cours sur le web</li> <li>Service bus – fournit de la communication interne dans l'écosystème Wanda</li> <li>Storage accounts – utilise pour conserver l'état de conversation et les paramètres utilisateur</li> <li>Cosmos DB –fournit du stockage</li> <li>Key vault – conserve des données confidentielles qui sont utilisées pour communiquer avec des services Microsoft et pour services internes</li> <li>Redis cache – fournit des capacités de cache</li> <li>Application Insights – supervision du système, y compris telemetrie et création d'incident</li> <li>SQL server – fournit du stockage</li> <li>Kubernetes – conteneur open source</li> </ul> <p>De plus amples informations et détails sur les produits et les services Microsoft peuvent être trouvés ici: <a href="https://azure.microsoft.com/en-us/services/">https://azure.microsoft.com/en-us/services/</a>.</p>
--	--	--

#### 4. PERIODE DE RETENTION

Le Sous-Traitant conservera les Données à Caractère Personnel pour la durée du Contrat.

Après la durée convenue de rétention, le Sous-Traitant restituera les Données à Caractère Personnel au Responsable de Traitement dans un format pouvant être migré défini par le Sous-Traitant ou détruira immédiatement les Données à Caractère Personnel sans conserver de copie, à première demande du Responsable de Traitement.

#### 5. INFORMATION CONCERNANT LE PAYS (OU LIEU) DE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Produit - Sur place	Les données sont conservées sur les serveurs du Responsable du Traitement au lieu d'activité principal ou au siège social qui est indiqué périodiquement à Unit4.		
Produit Services Cloud d'Unit4	Unit4 Cloud est exploité dans plusieurs centres de données, et est présent dans le monde entier via le partenariat Microsoft Azure. Unit4 déploiera le client sur le lieu le plus logique en fonction du lieu de résidence du client (indiqué dans le Bon de Commande). Toutes les données du client seront uniquement conservées dans la zone géopolitique sélectionnée et ne seront pas transférées en dehors de celle-ci sans le consentement explicite du client.		
	MODELE Cloud	ZONE	LOCALISATION DU CENTRE DE DONNEES
	SAAS CLOUD	UE	Dublin / Amsterdam
	SAAS CLOUD	USA	Localisations MULTIPLES
	SAAS CLOUD	CANADA	Toronto / VILLE DE Quebec
	SAAS CLOUD	ROYAUME UNI	LondRES / Cardiff
	SAAS CLOUD	ASIE	SingapoUR / Hong Kong
	SAAS CLOUD	AUSTRALIE	Victoria / New South Wales
	SAAS CLOUD	NORWAY	OSLO / STAVANGER
	SAAS CLOUD	SWEDEN (NORDICS)	SÅTRA AND SOLLENTUNA
Produit _ Gestion des Talent SaaS	Talent Management SaaS fonctionne dans le centre de données Amazon Web Services (AWS) à Francfort. Toutes les données des clients, à l'exception du partage avec les sous-traitants ultérieurs sélectionnés dans l'annexe 3, seront stockées uniquement dans la zone sélectionnée et ne seront pas déplacées en dehors de celle-ci sans le consentement explicite du client.		
Assistance Unit4 _ Assistance Standard et autres services d'assistance standard	L'Assistance Unit4 recourt au logiciel Salesforce pour enregistrer et traiter des Dossiers. Ces Dossiers sont accessibles par tout salarié Unit4 disposant d'un accès au logiciel Salesforce, par exemple les ingénieurs support, les ingénieurs cloud, les consultants et l'équipe de gestion des services des Services professionnels. L'accès est contrôlé par des processus de gestion et d'organisation internes, afin de s'assurer que l'accès aux Données à Caractère Personnel ne soit pas autorisé pour les consultants ou ingénieurs situés dans des pays ne devant pas avoir accès aux informations clients.		
	<b>Localisation du Client</b>	<b>Assistance principale fournie à partir des pays suivants:</b>	
	Royaume Uni et Irlande	Royaume Uni, Irlande, Portugal et Pologne.	

	Suède, Norvège, Danemark, Finlande et Islande	Pologne, Portugal, Norvège et Suède.		
	USA & Canada	Pologne, Portugal, USA et Canada.		
	Reste de l'Europe	Pologne, Portugal et Allemagne.		
	APAC	Pologne, Portugal et Singapour / Malaisie.		
Assistance Unit4 – Assistance 24 h/24 et 7 j./7 (Clients d'Assistance Renforcée et Premium)	Avec la mise en place de la méthode « suivre la course du soleil » (follow-the-sun), l'assistance 24 h/24 et 7 j/7 dans les Dossiers Clients peut intervenir depuis l'un quelconque des pays d'assistance susmentionnés..			
Assistance Unit4 – Assistance uniquement dans l'UE	Si l'option « Assistance uniquement dans l'UE » est retenue, les Dossiers seront uniquement soumis au service d'assistance dans les pays de l'UE susmentionnés pour l'assistance standard (pendant les heures de bureau).			
Les services People platform ("PPS") (en règle générale) comprenant IDS et Wanda (incluant tout service d'assistance associé)	Les services PPS sont des services cloud qui utilisent une infrastructure partagée et des services tiers qui peuvent s'étendre en dehors d'une zone géopolitique délimitée. Ci-dessous voici une présentation générale des services PPS et du pays (ou lieu) de Traitement de Données à Caractère Personnel en utilisant ces services.			
	<b>Service</b>	<b>Zone</b>	<b>Lieu où le Service Traite ou Conserve des Données</b>	<b>L'assistance est fournie principalement à partir de:</b>
	Wanda	Toute zone	Principalement au sein de l'UE, mais cela peut être ailleurs.	Irlande, USA et autres services d'assistance globaux, selon la demande
IDS	Dépend du déploiement du Cloud	Comme ci-dessus pour Unit4 SaaS	Comme ci-dessus pour SaaS	
Services Professionnels Unit4 et la fonction « customer success » d'Unit4	<b>Sujet</b>	<b>Les Services Professionnels et la fonction "customer success" sont fournis à partir de:</b>		
	Services d'implémentation et autres services liés à un projet	Sur le Territoire ou dans le pays du Client correspondant au siège social/principal établissement (suivant le cas) et/ou au Portugal en fonction de l'accord intervenu entre les Parties dans la documentation du projet ou un énoncé des travaux (suivant le cas).		
	Migration des données	Sur le Territoire ou dans le pays du Client correspondant au siège social/principal établissement (suivant le cas) et/ou au Portugal en fonction de l'accord intervenu entre les Parties dans la documentation du projet ou un énoncé des travaux (suivant le cas).		
	Dépannage	Dans le pays applicable suivant le « Service d'Assistance Unit4 » et au Portugal.		
Customer Success	Dans le pays applicable suivant le « Service d'Assistance Unit4 » et au Portugal.			

## 6. COORDONNEES

Pour toute question ou tout commentaire au sujet des présentes Conditions de Traitement de Données, veuillez joindre le point de contact suivant :

Le Responsable de Traitement peut adresser ses courriers au Sous-Traitant : par courrier (adressé au Global Data Privacy Officer, avec copie au Corporate Legal Department) P.O. Box 5005, 3528 BJ Utrecht, Pays-Bas ou par courriel à l'adresse [privacy@unit4.com](mailto:privacy@unit4.com) ou à l'adresse Unit4 indiquée aux fins de notification dans le Contrat.

Le Sous-Traitant peut adresser ses courriers au Responsable de Traitement: Adresse de notification du Responsable de Traitement indiquée dans le Contrat.

## ANNEXE 2 – MESURES DE SECURITE

Comme indiqué au paragraphe 6 des présentes Conditions de Traitement de Données, les mesures techniques et opérationnelles de sécurité sont listées dans la présente Annexe et sont complétées ou modifiées en cas de besoin. Le Responsable de Traitement considère que ces mesures sont adaptées pour le Traitement de Données à Caractère Personnel

### Unit4 Mesures de sécurité opérationnelles de Unit4 (résumé des opérations internes)

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le Sous-Traitant au sein de son organisation (en général):

#### **Sécurité physique :**

- Le contrôle d'accès physique est géré par les sites Unit4.
- Tous les bâtiments sont équipés de systèmes de sécurité contrôlant l'accès par des barrières, par exemple barrières d'accès aux entrées, réceptionnistes, portes coupe-feu munies de systèmes d'alarme, systèmes de détection d'intrusion et bureaux fermant à clé.
- Unit4 procède à des contrôles d'accès logique à l'aide d'informations détenues par le personnel (par exemple mots de passe et codes d'accès personnel), ou de dispositifs portés par celui-ci (par exemple un badge de sécurité).
- Les salles de serveurs sur site (le cas échéant) sont équipées de systèmes de contrôle physique supplémentaires.
- L'accès aux zones sécurisées ou aux informations sensibles est restreint pour empêcher l'accès non autorisé par les visiteurs/le personnel non autorisé (au moyen de bureaux ou d'armoires pouvant être fermés à clé et des politiques opérationnelles de « bureau vide » suivant les besoins).
- Les visiteurs Unit4 sont contrôlés à la réception (soit au moyen d'un réceptionniste attiré ou d'un autre membre du personnel).
- Des déchiqueteuses ou d'autres méthodes sûres de mise au rebut appropriées sont utilisées pour les documents sensibles.

#### **Sécurité virtuelle et informatique:**

- Le responsable hiérarchique garantira que les salariés et sous-traitants restitueront tous les biens Unit4 qui se trouvent en leur possession au moment de la résiliation de leur contrat de travail ou de prestation de services. Ces restitutions seront archivées dans le système de ticketing.
- Unit4 a pour but de catégoriser les informations sous les catégories « public », « confidentiel », « interne » ou « sensible ». Les informations seront ensuite protégées selon leur catégorie.
- Les supports (y compris les disques durs) qui ne sont plus utilisés sont éliminés en toute sécurité. Tous les matériels sensibles (disques durs, disquettes, etc.) sont supprimés par des logiciels de suppression garantis (autrement que par reformatage ou suppression) avant leur élimination ou la destruction physique.
- Anti-programmes malveillants – nous utilisons la toute dernière version des solutions standards du secteur d'activité pour offrir une protection contre les virus et les programmes malveillants.
- Par ailleurs, Unit4 utilise :
  - des modes de contrôle des droits attribués;
  - des mécanismes de connexion et de contrôle de l'accès au système;
  - des mesures de rétablissement ;
  - la capacité de garantir continuellement la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de Traitement ; et
  - des systèmes et processus lui permettant de restaurer rapidement la disponibilité des Données à Caractère Personnel et l'accès à celles-ci en cas d'incident physique ou technique.
- Le plan de poursuite des activités et le plan de reprise d'activité qui sont établis incluent des éléments de sécurité de l'information.

#### **Politiques de sécurité et documentation y afférente:**

- L'Équipe de Direction Globale (Global Leadership Team) de Unit4 et/ou ses équipes respectives de direction locale ont approuvé la gestion de l'information et les plans de sécurité, globaux et locaux, y compris toutes politiques de sécurité de l'information qui répondent aux risques identifiés de sécurité de l'information et soutiennent les objectifs de l'entreprise.
- La sécurité et la gestion de l'information sont attribuées au niveau mondial au Directeur Monde de la Sécurité de l'Information et au Directeur Monde de la Protection des Données qui gèrent les ressources de manière à respecter d'un point de vue global et stratégique la politique et les procédures de sécurité de l'information.
- Unit4 a mis en œuvre des politiques de sécurité qu'elle met à jour et modifie régulièrement pour respecter les bonnes pratiques du secteur d'activité.
- Unit4 a une politique de protection de la vie privée et un livre blanc sur le RGPD publiés à [www.unit4.com/about/ethics](http://www.unit4.com/about/ethics).
- Dans le cadre du partage d'informations confidentielles ayant trait à ses activités, Unit4 conclut des accords de confidentialité avec des Tiers.
- Unit4 veille à ce que tous les salariés et les sous-traitants concluent des contrats assortis de clauses de confidentialité.
- Unit4 dispense à tous les salariés une formation dans le cadre de la protection des données, de la sécurité et de tous les principes généraux de conduite des affaires qui sont indiqués ci-dessus.

### Éléments supplémentaires concernant les Services Unit4 (résumé)

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le Sous-Traitant dans le cadre de la fourniture des Services Unit4 Cloud :

#### **Protection des données**

Unit4 Cloud recourt à plusieurs mécanismes de protection des Données à Caractère Personnel dans le cloud. Ci-après figure un aperçu des dispositifs de contrôle appliqués.

#### Caractéristiques, processus et protocoles de sécurité au niveau du réseau

- Transmission sécurisée de données dans les réseaux publics – tout le trafic est sécurisé à l'aide des protocoles standard du secteur d'activité, par exemple SSL/TLS et HTTPS.
- Sécurité des systèmes – authentification logique et mécanisme d'autorisation en place.

- Pare-feu – technologie de pare-feu de nouvelle génération garantissant le contrôle du trafic entrant et sortant.

#### Caractéristiques, processus et protocoles de sécurité au niveau des bases de données

- Sécurité des données – authentification logique et mécanisme d'autorisation en place.
- Sécurité des bases de données – chaque client possède sa propre base de données sécurisée, ce qui signifie qu'aucun cloisonnement des bases de données n'est requis et que les données des clients ne sont pas mélangées. Par conséquent, les données d'un client ne sont jamais partagées par inadvertance avec celles d'autrui.
- Les copies de sauvegarde sont chiffrées à l'aide d'une technologie de chiffrement des bases de données comme le Chiffrement Transparent des Bases de données. Fonctionnalité de chiffrement des données au repos d'Azure utilisée pour chiffrer toutes les données placées dans le compte de stockage d'un client.
- Unit4 utilise la fonctionnalité de coffre-fort de clés d'Azure (« Azure Key Vault ») pour conserver le contrôle des clés utilisées dans les applications et services cloud pour chiffrer les données.

#### Une sécurité continuellement testée et en évolution

Pour découvrir les failles imprévues et affiner nos capacités de détection et de réaction, nous recherchons continuellement des manières d'améliorer notre niveau de sécurité afin de nous défendre contre lesdites failles éventuelles. L'équipe opérationnelle Unit4 Cloud qui surveille de près et sécurise les opérations Unit4 Cloud (infrastructure sur le cloud, services cloud, produits, appareils et ressources internes) simule des failles réelles, tout en effectuant des tests de pénétration et en améliorant notre capacité à nous protéger contre les cyberattaques, à détecter celles-ci et reprendre nos activités après une cyberattaque.

#### Détection et réduction des menaces et réaction face à celles-ci

Du fait de l'augmentation du nombre, de la diversité et de la gravité des cyberattaques, nous avons augmenté nos diligences dans les domaines de la détection des menaces et de la réaction face à celles-ci. Des systèmes de contrôle centralisés offrent une visibilité continue et des alertes en temps réel. L'application fréquente de patches et de mises à jour de sécurité contribue à protéger les systèmes des vulnérabilités connues. Les systèmes de détection des intrusions et des programmes malveillants sont conçus pour détecter et réduire les risques provenant des attaques extérieures. En cas d'activités malveillantes, notre équipe en charge des incidents, suit des procédures établies pour gérer et communiquer les incidents et assurer la reprise des activités après un incident. L'équipe applique les meilleures pratiques du secteur d'activité pour prévenir les équipes internes et les clients. Enfin, les rapports de sécurité surveillent les modèles d'accès pour contribuer à identifier et réduire les menaces potentielles en amont.

#### Séparation des données

Les données sont la monnaie d'échange de l'économie numérique et nous prenons nos responsabilités très au sérieux pour protéger les données de nos clients. Des mesures de sécurité techniques, par exemple le chiffrement des communications et des processus opérationnels, contribuent à sécuriser les données de nos clients. Dans le Cloud, les données de nos nombreux clients peuvent être conservées sur les mêmes ressources informatiques. Unit4 utilise l'isolement logique pour séparer les données de chaque client et celles des autres clients. La solution SaaS de Unit4 est conçue pour lutter contre les risques inhérents à un environnement multilocataires. La conservation et le traitement des données bénéficient d'une séparation logique entre les consommateurs, à l'aide par exemple de Comptes Dédiés et d'instances distinctes de bases de données pour tous nos clients.

#### Isolement du réseau à plusieurs points:

- Chaque déploiement dédié est isolé des autres déploiements et leur communication est assurée par des adresses IP privées.
- Les machines virtuelles du Client peuvent uniquement communiquer avec d'autres machines virtuelles détenues ou contrôlées par le même Client et équipées de points de terminaison de services d'infrastructure conçus pour les communications publiques.
- Le trafic entre les machines virtuelles passe toujours par des filtres de paquets approuvés.

Pour des détails supplémentaires sur la Politique de Sécurité et le Programme de Sécurité, veuillez consulter [www.unit4.com/terms](http://www.unit4.com/terms).

#### **Chiffrement des données**

Unit4 offre par défaut un accès sécurisé à tous ses services où toutes les données en transit sur des réseaux publics sont chiffrées. Le chiffrement est effectué à l'aide uniquement de protocoles sûrs, comme HTTPS sur TLS, à l'aide des toutes dernières méthodes de chiffrement. Les clients ont le choix de commander sur option le chiffrement des « données au repos ». Le mécanisme utilisé est un chiffrement transparent de toute la base de données, « TDE ». Les clients Microsoft Azure de l'offre Public SaaS obtiennent par défaut le chiffrement TDE des données au repos.

#### **Contrôle des accès**

Les Clients qui utilisent les Produits Unit4 dans le Cloud ont pleinement le pouvoir de contrôler l'accès front-end de leur application. En d'autres termes, la responsabilité de créer de nouveaux comptes, de résilier des comptes et de revoir l'application Unit4 appartient au Client.

Unit4 conserve un accès back-end limité aux données du client (par connexion directe aux bases de données). L'accès de Unit4 à des informations personnelles sera strictement limité aux activités nécessaires pour installer, implémenter, maintenir, réparer, dépanner ou mettre à niveau la solution. Tous les accès sont journalisés et limités à un groupe restreint d'Ingénieurs Cloud et de Consultants Assistance. Les journaux des accès sont sauvegardés dans la solution de contrôle centralisée pendant 365 jours. En cas de violations de données, Unit4 peut fournir le journal d'accès sur demande.

#### **Notification en cas de violation de données**

Unit4 notifiera toute violation de données au Client dans les meilleurs délais après en avoir eu connaissance. Le Client doit veiller à tenir à jour en permanence les coordonnées des personnes indiquées sur le Portail d'Assistance Unit4 car elles serviront pour toutes les communications.

#### **Protection des données et sécurité dès la conception**

La plateforme Unit4 Cloud a été conçue en gardant sans cesse à l'esprit les principes de sécurité et protection des données. Unit4 améliore continuellement la sécurité de la solution, en appliquant les enseignements tirés des tests d'intrusion et audits annuels.

À titre de preuve de la conception et des opérations dans une optique de sécurité, les opérations SaaS des Services Unit4 Cloud détiennent la certification ISO 27001:2013 et a obtenu le rapport ISAE3402 (SOC1). Unit4 et les opérateurs de centres de données détiennent plusieurs certifications de sécurité dont les détails figurent dans la Description des Services Cloud

#### [Éléments supplémentaires pour les services People Platform Services d'Unit4 \(résumé\)](#)

Description des mesures de sécurité techniques et opérationnelles mises en œuvre par le Sous-Traitant en ce qui concerne la fourniture des services People Platform Services d'Unit4 (Cloud uniquement):

### Protection des données

La People Platform d'Unit4 utilise plusieurs mécanismes de protection des Données à Caractère Personnel dans le cloud. Ci-dessous une présentation complète des contrôles mis en place.

Caractéristiques, processus et protocoles de sécurité au niveau du réseau

- Transmission sécurisée des données dans les réseaux publics – tout le trafic est sécurisé à l'aide des protocoles standard du secteur d'activité, par exemple SSL/TLS (1.2) et HTTPS.

### Authentification

- Tous les services suivent le principe du moindre privilège et de l'authentification envers les services et leurs APIs sont sécurisées selon les mécanismes standard du secteur d'activité. OpenID Connect et le protocole sous-jacent OAuth 2.0 est utilisé pour effectuer l'authentification sécurisée des utilisateurs et/ou des services clients avec des tiers approuvés et pour valider l'identité et l'accès en utilisant des tokens sur demande.
- HMAC (Hash-based Message Authentication) est utilisé comme méthode alternative pour sécuriser la communication entre services.

Caractéristiques, processus et protocoles de sécurité au niveau des bases de données.

- La donnée conservée dans des comptes de sauvegarde sont chiffrées au repos .
- Tous les comptes de sauvegarde requièrent un transfert sécurisé – tout le trafic est sécurisé selon les protocoles standard du secteur d'activité, tels que SSL/TLS et HTTPS.
- Toutes les données stockées dans Azure Cosmos DB sont chiffrées au repos et en transit .
- Tous les serveurs Azure SQL sont activés avec le Chiffrement Transparent de Données (« Transparent Data Encryption (TDE) »).
- Tous les serveurs Azure SQL fonctionnent avec la détection de Menace et peuvent être audités.
- Azure KeyVault est utilisé pour la sécurisation des informations particulièrement sensibles telles que les identifiants principaux de comptes de service.

Caractéristiques, processus et protocoles de sécurité au niveau de la messagerie.

- Toutes les données stockées par instances Azure Service Bus sont chiffrées au repos.
- Tout le trafic (en transit) sur Azure Service Bus est sécurisé selon les protocoles standard du secteur d'activité tels que SSL.

Pour de plus amples informations et détails sur la Politique de Sécurité et le Programme de Sécurité, voir [www.unit4.com/terms](http://www.unit4.com/terms).

### Chiffrement de données

People Platform Services d'Unit4 fournit, par défaut, un accès sécurisé à tous ses services en chiffrant toutes les données en transit sur des réseaux publics. Le chiffrement est effectué à l'aide uniquement de protocoles sûrs, tels que HTTPS sur TLS (1.2), à l'aide des toutes dernières méthodes de chiffrement. Toutes les données conservées sont chiffrées.

### Notification en cas de violation de données

Unit4 notifiera toute violation de données au Client dans les meilleurs délais après en avoir eu connaissance. Le Client doit veiller à tenir à jour en permanence les coordonnées des personnes indiquées sur le Portail d'Assistance d'Unit4 car elles serviront pour toutes communications.

### Protection des données et sécurité dès la conception

La plateforme People Platform d'Unit4 a été conçue en gardant sans cesse à l'esprit les principes de sécurité et protection des données. Unit4 améliore continuellement la sécurité de la solution, en appliquant les enseignements tirés des tests d'intrusion et audits annuels.

### Éléments supplémentaires pour les Services Gestion des Talents d'Unit4 – SaaS (résumé)

La Gestion des Talents SaaS est certifié ISO27001 et a passé un audit ISO27001 (phase 1 & 2) et RGPD. Le tableau ci-dessous relate les points essentiels, une documentation supplémentaire ou information supplémentaire est disponible à la demande.

Domaine	Pratiques
Sécurité, gestion et gouvernance de l'information	Le service de Gestion des Talents SaaS a mis en œuvre un système de Gestion de la Sécurité de l'Information (Information Security Management System (ISMS)) au sens de ISO27001. Il comprend, sans limitation, une politique de sécurité de l'information adressée à tous les salariés. La politique est disponible sur demande. En outre, afin de fournir la sécurité de l'information, des mesures de gestion sont mises en œuvre qui minimisent les risques. Ces risques et la plausibilité qu'ils se réalisent sont inclus dans le ISO27001 ISMS.
Sécurité des Ressources Humaines	La fourniture de services de Gestion des Talents SaaS permet de conserver toutes les données confidentielles dans un système d'information des ressources humaines (« HRIS ») et de se conformer à ISO27001 et pour lequel le département de la sécurité de l'information est responsable.
Gestion des biens	Les biens (tangibles et intangibles) sont maintenus en fonction d'une politique de catégorisation de données.
Contrôle d'accès à l'information	Il existe plusieurs politiques qui appliquent le principe du moindre privilège, à la fois pour les applications fournies, les informations générales et les propres données. L'accès à ses propres systèmes, hébergés sur Amazon (AWS) est restreint à des personnes spécifiquement identifiées et l'utilisation de mots de passe est expressément interdit. Seuls les couples de clés publique / privé sont utilisées pour s'authentifier sur les serveurs.

Les droits d'accès par utilisateur sont déterminés en accord avec la politique d'accès établie. Les questions spécifiques sur l'accès à l'information et les politiques qui y sont relatives peuvent être dirigées vers l'équipe en charge de la sécurité de l'information.

---

Sécurité des Opérations    Ceci est traité dans l'ISMS (ISO27001).

---

Sécurité des Communications    Toute communication fait l'objet d'une politique de catégorisation de données. Tout trafic réseau s'effectue sur SSL/HTTPS, le protocole de communication sur internet le plus communément accepté. L'infrastructure interne est isolée en utilisant des pare-feux stricts et des listes d'accès au réseau. Chaque système est dédié à un groupe de pare-feu de sécurité par fonction. Par défaut, tous les accès sont refusés et seuls des ports agréés expressément sont exposés. Les "layers" de Persistence et de stockage sont chiffrés (également au repos) et sécurisés par des pare-feux VPN & VPC.

Les bureaux utilisent un réseau protégé par un pare-feu redondant Fortinet 200D, situé dans le centre de données de Merelbeke, connecté au Ghelamco Arena via Dark Fiber. De plus amples informations à propos de cette connection sont fournies dans le document intitulé Mesures de continuité et de sécurité ("Continuity and Security measures") et qui fait partie du ISMS de la certification ISO27001 .

---

## ANNEXE 3 - SOUS-TRAITANTS ULTERIEURS D'UNIT4

Service	Sous-Traitant Ulérieur (raison sociale, lieu de la société, etc)	Lieu du Traitement	Type de service par Sous-Traitant Ulérieur / Module utilisé
Services Professionnels Unit4 (si sous-traités à un partenaire en charge de la livraison)	Cf. Contrat.	Cf. Contrat.	Cf. Bon de commande ou accord écrit avec le Client.
Produits et Services Tiers uniquement applicables lorsqu'ils sont achetés par le client	Cf. Contrat	Cf. Contrat ou toute autre annexe ou tout autre appendice relatifs au traitement du Fournisseur tiers	Services Logiciels et/ou d'Assistance et/ou Services Cloud
Services SaaS	Microsoft Azure	voir les indications ci-dessus à l'Annexe 2, paragraphe 5.	Fourniture d'infrastructure Cloud et Services Cloud
	Microsoft Dynamics	voir les indications ci-dessus à l'Annexe 2, paragraphe 5.	Fourniture de Services Logiciels, en particulier Microsoft Dynamics (y compris certaines infrastructures cloud).
	Microsoft	voir les indications ci-dessus à l'Annexe 2, paragraphe 5.	Fourniture d'outils logiciels et Office
	Conapto	voir les indications ci-dessus à l'Annexe 2, paragraphe 5..	Fourniture d'infrastructures et de services Cloud
Services Cloud d'Unit4 – Gestion des Talents	Amazon Web Services	Francofort, Allemagne	Fourniture de solution - Suite
	Freshdesk	USA (Privacy Policy)	Fourniture de solution – Suite (lien vers le privacy shield : Link)
	LogDNA	USA (Privacy Policy)	Fourniture de solution – Suite (lien vers le privacy shield: Link)
	Mandrill	USA (Privacy Policy)	Fourniture de solution – Suite (lien vers le privacy shield: Link)
	Mixpanel	USA (Privacy Policy)	Fourniture de solution – Suite (lien vers le privacy shield: Link)
	Pingdom	USA (Privacy Policy)	Fourniture de solution – Suite (lien vers le privacy shield: Link)
	Produitboard	Espace Economique Européen et USA (Privacy Policy)	Fourniture de solution – Suite (lien vers le privacy shield: Link)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Fourniture de solution è - Learn (SCORM uniquement) (lien vers le privacy shield : Link)
	Sentry	USA (Privacy Policy)	Fourniture de solution – Suite (lien vers le privacy shield: Link)
	Slack	USA (Privacy Policy)	Fourniture de solution – Perform (lien vers le privacy shield : Link)
	Stripe	pays où Stripe est actif (Privacy Policy)	Fourniture de solution – Learn (lien vers le privacy shield : Link)
	Wistia	USA (Privacy Policy)	Fourniture de solution – Learn (lien vers le privacy shield : Link)
People Platform Services ("PPS") (en règle générale) comprenant IDS et Wanda (incluant tout service d'assistance associé)	Microsoft Azure	Cf. indications ci-dessus à l'Annexe 1, paragraphe 5 et tel que décrit par Microsoft ici: <a href="https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located">https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located</a> .	Fourniture d'infrastructure et services de plateforme Cloud (tel que décrit ci-dessus) à la section 2

## ANNEXE 4 – CLAUSES CONTRACTUELLES TYPES DE L'UE

Ce tableau comprend l'information requise devant être insérée dans les Clauses contractuelles type de l'UE qui sont détaillées en dessous du présent tableau:

<b>Parties</b>	L'exportateur de données est le Responsable de Traitement dont les coordonnées apparaissent dans un Bon de commande (en tant que Client) dans le Contrat entre le Responsable de Traitement et le Sous-Traitant.  L'importateur de données est le Sous-Traitant dont les coordonnées apparaissent dans un Bon de commande (en tant que Unit4) dans le Contrat entre le Responsable de Traitement et le Sous-Traitant,
<b>Clause 9 and 11(3)</b>	L'exportateur de données est situé dans le Territoire indiqué dans le Contrat.
<b>Appendice 1</b>	L'information demandée pour remplir cet appendice est détaillée en Annexe 1 et Annexe 3 des présentes Conditions de Traitement de Données
<b>Appendice 2</b>	L'information demandée pour remplir cet appendice est détaillée en Annexe 2 des présentes Conditions de Traitement de Données

## CLAUSES CONTRACTUELLE TYPES (SOUS-TRAITANTS)

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

Parties

Nom de l'organisation exportant les données:

Adresse:

Tél .....; fax .....; courrier électronique: .....

Autres informations nécessaires pour identifier l'organisation:

....

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

d'une part, et

Nom de l'organisation important les données:

Adresse: .....

Tél.:..... ; fax:..... ; courrier électronique:

Autres informations nécessaires pour identifier l'organisation:

(ci-après dénommée l'«**importateur de données**»)

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

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

### Clause 1

#### Définitions

Au sens des clauses:

- a) «données à caractère personnel», «catégories particulières de données», «traiter/traitement», «responsable du traitement», «sous-traitant», «personne concernée» et «autorité de contrôle» ont la même signification que dans la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données<sup>1</sup>;
- b) l'«exportateur de données» est le responsable du traitement qui transfère les données à caractère personnel;
- c) l'«importateur de données» est le sous-traitant qui accepte de recevoir de l'exportateur de données des données à caractère personnel destinées à être traitées pour le compte de ce dernier après le transfert conformément à ses instructions et aux termes des présentes clauses et qui n'est pas soumis au mécanisme d'un pays tiers assurant une protection adéquate au sens de l'article 25, paragraphe 1, de la directive 95/46/CE;
- d) le «sous-traitant ultérieur» est le sous-traitant engagé par l'importateur de données ou par tout autre sous-traitant ultérieur de celui-ci, qui accepte de recevoir de l'importateur de données ou de tout autre sous-traitant ultérieur de celui-ci des données à caractère personnel exclusivement destinées à des activités de traitement à effectuer pour le compte de l'exportateur de données après le transfert conformément aux instructions de ce dernier, aux conditions énoncées dans les présentes clauses et selon les termes du contrat de sous-traitance écrit;
- e) le «droit applicable à la protection des données» est la législation protégeant les libertés et les droits fondamentaux des personnes, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans l'État membre où l'exportateur de données est établi;
- f) les «mesures techniques et d'organisation liées à la sécurité» sont les mesures destinées à protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement.

### Clause 2

#### Détails du transfert

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

### Clause 3

#### Clause du tiers bénéficiaire

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

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

2. La personne concernée peut faire appliquer contre l'importateur de données la présente clause, ainsi que la clause 5, points a) à e) et g), la clause 6, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12 dans les cas où l'exportateur de données a matériellement disparu ou a cessé d'exister en droit, à moins que l'ensemble de ses obligations juridiques ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, à laquelle reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre laquelle la personne concernée peut donc faire appliquer lesdites clauses.
3. La personne concernée peut faire appliquer contre le sous-traitant ultérieur la présente clause, ainsi que la clause 5, points a) à e) et g), la clause 6, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12, mais uniquement dans les cas où l'exportateur de données et l'importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvable, à moins que l'ensemble des obligations juridiques de l'exportateur de données ait été transféré, par contrat ou par effet de la loi, au successeur légal, auquel reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre lequel la personne concernée peut donc faire appliquer lesdites clauses. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.
4. Les parties ne s'opposent pas à ce que la personne concernée soit représentée par une association ou un autre organisme si elle en exprime le souhait et si le droit national l'autorise.

#### **Clause 4**

##### **Obligations de l'exportateur de données**

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

- a) le traitement, y compris le transfert proprement dit des données à caractère personnel, a été et continuera d'être effectué conformément aux dispositions pertinentes du droit applicable à la protection des données (et, le cas échéant, a été notifié aux autorités compétentes de l'État membre dans lequel l'exportateur de données est établi) et n'enfreint pas les dispositions pertinentes dudit État;
- b) il a chargé, et chargera pendant toute la durée des services de traitement de données à caractère personnel, l'importateur de données de traiter les données à caractère personnel transférées pour le compte exclusif de l'exportateur de données et conformément au droit applicable à la protection des données et aux présentes clauses;
- c) l'importateur de données offrira suffisamment de garanties en ce qui concerne les mesures techniques et d'organisation liées à la sécurité spécifiées dans l'appendice 2 du présent contrat;
- d) après l'évaluation des exigences du droit applicable à la protection des données, les mesures de sécurité sont adéquates pour protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement et elles assurent un niveau de sécurité adapté aux risques liés au traitement et à la nature des données à protéger, eu égard au niveau technologique et au coût de mise en œuvre;
- e) il veillera au respect des mesures de sécurité;
- f) si le transfert porte sur des catégories particulières de données, la personne concernée a été informée ou sera informée avant le transfert ou dès que possible après le transfert que ses données pourraient être transmises à un pays tiers n'offrant pas un niveau de protection adéquat au sens de la directive 95/46/CE;
- g) il transmettra toute notification reçue de l'importateur de données ou de tout sous-traitant ultérieur conformément à la clause 5, point b), et à la clause 8, paragraphe 3), à l'autorité de contrôle de la protection des données s'il décide de poursuivre le transfert ou de lever sa suspension;
- h) il mettra à la disposition des personnes concernées, si elles le demandent, une copie des présentes clauses, à l'exception de l'appendice 2, et une description sommaire des mesures de sécurité, ainsi qu'une copie de tout contrat de sous-traitance ultérieure ayant été conclu conformément aux présentes clauses, à moins que les clauses ou le contrat contienne(nt) des informations commerciales, auquel cas il pourra retirer ces informations;
- i) en cas de sous-traitance ultérieure, l'activité de traitement est effectuée conformément à la clause 11 par un sous-traitant ultérieur offrant au moins le même niveau de protection des données à caractère personnel et des droits de la personne concernée que l'importateur de données conformément aux présentes clauses; et
- j) il veillera au respect de la clause 4, points a) à i).

#### **Clause 5**

##### **Obligations de l'importateur de données<sup>2</sup>**

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

- a) il traitera les données à caractère personnel pour le compte exclusif de l'exportateur de données et conformément aux instructions de ce dernier et aux présentes clauses; s'il est dans l'incapacité de s'y conformer pour quelque raison que ce soit, il accepte d'informer dans les meilleurs délais l'exportateur de données de son incapacité, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat;
- b) il n'a aucune raison de croire que la législation le concernant l'empêche de remplir les instructions données par l'exportateur de données et les obligations qui lui incombent conformément au contrat, et si ladite législation fait l'objet d'une modification susceptible d'avoir des conséquences négatives importantes pour les garanties et les obligations offertes par les clauses, il communiquera la modification à l'exportateur de données sans retard après en avoir eu connaissance, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat;
- c) il a mis en œuvre les mesures techniques et d'organisation liées à la sécurité spécifiées dans l'appendice 2 avant de traiter les données à caractère personnel transférées;
- d) il communiquera sans retard à l'exportateur de données:
  - i) toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre, sauf disposition contraire, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière;
  - ii) tout accès fortuit ou non autorisé; et

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

- iii) toute demande reçue directement des personnes concernées sans répondre à cette demande, à moins qu'il n'ait été autorisé à le faire;
- e) il traitera rapidement et comme il se doit toutes les demandes de renseignements émanant de l'exportateur de données relatives à son traitement des données à caractère personnel qui font l'objet du transfert et se rangera à l'avis de l'autorité de contrôle en ce qui concerne le traitement des données transférées;
- f) à la demande de l'exportateur de données, il soumettra ses moyens de traitement de données à une vérification des activités de traitement couvertes par les présentes clauses qui sera effectuée par l'exportateur de données ou un organe de contrôle composé de membres indépendants possédant les qualifications professionnelles requises, soumis à une obligation de secret et choisis par l'exportateur de données, le cas échéant, avec l'accord de l'autorité de contrôle;
- g) il mettra à la disposition de la personne concernée, si elle le demande, une copie des présentes clauses, ou tout contrat de sous-traitance ultérieure existant, à moins que les clauses ou le contrat contienne(nt) des informations commerciales, auquel cas il pourra retirer ces informations, à l'exception de l'appendice 2, qui sera remplacé par une description sommaire des mesures de sécurité, lorsque la personne concernée n'est pas en mesure d'obtenir une copie de l'exportateur de données;
- h) en cas de sous-traitance ultérieure, il veillera au préalable à informer l'exportateur de données et à obtenir l'accord écrit de ce dernier;
- i) les services de traitement fournis par le sous-traitant ultérieur seront conformes à la clause 11;
- j) il enverra dans les meilleurs délais une copie de tout accord de sous-traitance ultérieure conclu par lui en vertu des présentes clauses à l'exportateur de données.

## **Clause 6**

### **Responsabilité**

1. Les parties conviennent que toute personne concernée ayant subi un dommage du fait d'un manquement aux obligations visées à la clause 3 ou à la clause 11 par une des parties ou par un sous-traitant ultérieur a le droit d'obtenir de l'exportateur de données réparation du préjudice subi.
2. Si une personne concernée est empêchée d'intenter l'action en réparation visée au paragraphe 1 contre l'exportateur de données pour manquement par l'importateur de données ou par son sous-traitant ultérieur à l'une ou l'autre de ses obligations visées à la clause 3 ou à la clause 11, parce que l'exportateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'importateur de données accepte que la personne concernée puisse déposer une plainte à son encontre comme s'il était l'exportateur de données, à moins que l'ensemble des obligations juridiques de l'exportateur de données ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, contre laquelle la personne concernée peut alors faire valoir ses droits.
3. L'importateur de données ne peut invoquer un manquement par un sous-traitant ultérieur à ses obligations pour échapper à ses propres responsabilités.
4. Si une personne concernée est empêchée d'intenter l'action visée aux paragraphes 1 et 2 contre l'exportateur de données ou l'importateur de données pour manquement par le sous-traitant ultérieur à l'une ou l'autre de ses obligations visées à la clause 3 ou à la clause 11, parce que l'exportateur de données et l'importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolubles, le sous-traitant ultérieur accepte que la personne concernée puisse déposer une plainte à son encontre en ce qui concerne ses propres activités de traitement conformément aux présentes clauses comme s'il était l'exportateur de données ou l'importateur de données, à moins que l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données ait été transféré, par contrat ou par effet de la loi, au successeur légal, contre lequel la personne concernée peut alors faire valoir ses droits. La responsabilité du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

## **Clause 7**

### **Médiation et juridiction**

1. L'importateur de données convient que si, en vertu des clauses, la personne concernée invoque à son encontre le droit du tiers bénéficiaire et/ou demande réparation du préjudice subi, il acceptera la décision de la personne concernée:
  - a) de soumettre le litige à la médiation d'une personne indépendante ou, le cas échéant, de l'autorité de contrôle;
  - b) de porter le litige devant les tribunaux de l'État membre où l'exportateur de données est établi.
2. Les parties conviennent que le choix effectué par la personne concernée ne remettra pas en cause le droit procédural ou matériel de cette dernière d'obtenir réparation conformément à d'autres dispositions du droit national ou international.

## **Clause 8**

### **Coopération avec les autorités de contrôle**

1. L'exportateur de données convient de déposer une copie du présent contrat auprès de l'autorité de contrôle si celle-ci l'exige ou si ce dépôt est prévu par le droit applicable à la protection des données.
2. Les parties conviennent que l'autorité de contrôle a le droit d'effectuer des vérifications chez l'importateur de données et chez tout sous-traitant ultérieur dans la même mesure et dans les mêmes conditions qu'en cas de vérifications opérées chez l'exportateur de données conformément au droit applicable à la protection des données.
3. L'importateur de données informe l'exportateur de données dans les meilleurs délais de l'existence d'une législation le concernant ou concernant tout sous-traitant ultérieur faisant obstacle à ce que des vérifications soient effectuées chez lui ou chez tout sous-traitant ultérieur conformément au paragraphe 2. Dans ce cas, l'exportateur de données a le droit de prendre les mesures prévues par la clause 5, point b).

## **Clause 9**

### **Droit applicable**

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

## **Clause 10**

### **Modification du contrat**

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

## **Clause 11**

### **Sous-traitance ultérieure**

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

Le contrat écrit préalable entre l'importateur de données et le sous-traitant ultérieur prévoit également une clause du tiers bénéficiaire telle qu'énoncée à la clause 3 pour les cas où la personne concernée est empêchée d'intenter l'action en réparation visée à la clause 6, paragraphe 1, contre l'exportateur de données ou l'importateur de données parce que ceux-ci ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolubles, et que l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données n'a pas été transféré, par contrat ou par effet de la loi, à une autre entité leur ayant succédé. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

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

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

## **Clause 12**

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

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

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

Les parties conviennent que les présentes Clauses Contractuelles Types deviennent obligatoires lors de la conclusion d'un bon de commande de services entre les parties, qui forment un contrat.

## **Appendice 1**

### **Aux Clauses Contractuelles Types**

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

Les États membres peuvent compléter ou préciser, selon leurs procédures nationales, toute information supplémentaire devant éventuellement être incluse dans le présent appendice.

### **Exportateur de données**

L'exportateur de données est (veuillez préciser brièvement vos activités qui présentent un intérêt pour le transfert):

Cf. Annexe 1 des Conditions de Traitement de Données (ci-dessus).

### **Importateur de données**

L'importateur de données est (veuillez préciser brièvement vos activités qui présentent un intérêt pour le transfert):

Cf. Annexe 1 des Conditions de Traitement de Données (ci-dessus).

### **Personnes concernées**

Les données à caractère personnel transférées concernent les catégories suivantes de personnes concernées (veuillez préciser):

Cf. Annexe 1 des Conditions de Traitement de Données (ci-dessus).

### **Catégories de données**

Les données à caractère personnel transférées concernent les catégories suivantes de données (veuillez préciser):

Cf. Annexe 1 des Conditions de Traitement de Données (ci-dessus).

### **Catégories particulières de données (le cas échéant)**

Les données à caractère personnel transférées concernent les catégories particulières suivantes de données (veuillez préciser):

Cf. Annexe 1 des Conditions de Traitement de Données (ci-dessus).

### **Traitement**

Les données à caractère personnel transférées seront soumises aux activités de traitement de base suivantes (veuillez préciser):

Cf. Annexe 1 des Conditions de Traitement de Données (ci-dessus).

<sup>3</sup> Cette condition peut être réputée remplie si le sous-traitant ultérieur est co-signataire du contrat conclu entre l'exportateur de données et l'importateur de données conformément à la présente décision.

## Appendice 2

### Aux clauses contractuelles types

**Description des mesures de sécurité techniques et organisationnelles mises en œuvre par l'importateur de données conformément aux clauses 4(d) et 5(c) (ou document/législation jointe) :**

Voir l'annexe 2 des conditions de traitement des données (ci-dessus).