

SECTION 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 x	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 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 bancaire; 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 pas nécessaire 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	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. 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. En utilisant le module « Perform » : données d'enregistrement, données relatives aux objectifs et résultats clés (OKR), retours et évaluations. En utilisant le module « Engage » : réponses et retours sur les questions d'implication de l'employé.	Anciens membres du personnel et membres actuels Anciens candidats à l'embauche et candidats actuels; Prestataires ou sous-traitants (de quelque forme que ce soit) agents ou dirigeants; et Candidats à l'embauche ou salariés potentiels.
People Platform Services ("PPS"), Services de Localisation et Unit4 Apps	Etant donné que les PPS, les services de Localisation et/ou les Unit4 Apps fonctionnent et s'interfaçent 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. 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).	Toutes les personnes physiques listées dans le présent tableau. 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.
Unit4 Property Management	Noms; adresses; numéros de téléphone (y compris portable); adresse électronique; adresse de la page web; numéro de sécurité sociale ou numéro de sécurité nationale ou référence de carte d'identité; date de naissance; identité du Client; langue(s) parlée(s); identification d'identité protégée; identification du bien; numéro de TVA; informations sur les personnes de contact (y compris le titre / le rôle, les intérêts); les coordonnées bancaires; les informations sur l'emploi (y compris : employeur, adresse); coordonnées du candidat (y compris : profession, revenu annuel; année d'embauche; nombre de personnes dans le foyer; propriétaire précédent; évaluation du rapport de crédit; date de l'évaluation de crédit); candidat et autres attributs (définis par le Responsable de Traitement); rang dans la liste; qualité de membre (y compris numéro d'adhésion, statut; date et fin de l'adhésion, points attribués comme preneur, points sur l'épargne personnelle); rôles/ catégories de personnes; Utilisateurs (identifiant d'utilisateur, type d'utilisateur, signature); contrat de bail et détails sur l'association et/ou syndic de copropriété (y compris : identité du destinataire des factures pour les factures électroniques; information relative au mandat de dépôt de garantie, garant, garanties); renseignements sur la gestion de Dossiers; prestataire/entrepreneur (mandats pour l'envoi de courriel); Notes (enregistrées par le Responsable de Traitement); documents (écrits ou électroniques) contenant l'un des éléments ci-dessus.	Anciens membres du personnel et membres actuels; Entrepreneurs ou Sous-traitants (de tout type), agents ou dirigeants; Candidats ou prospects; et les consommateurs de services managés (par exemple les candidats à la propriété et les locataires)

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 au Contrat, 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. Le Sous-Traitant Traitera vos Données à Caractère Personnel pour l'amélioration de ses produits et services (par exemple pour l'amélioration de produit par intelligence artificielle, machine learning etc) ou pour l'analyse de données.

Dans le cadre et en fonction du Produit ou du Service, le Traitement comprendra ce qui suit :

Produit	Nature et finalité du traitement
Unit4 ERP x	Les Données à Caractère Personnel seront saisies dans Unit4 ERP 8, 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 : <ul style="list-style-type: none"> • les demandes de déplacements ; • le traitement des demandes de remboursement de frais ;

	<ul style="list-style-type: none"> • le traitement des feuilles de présence ; • la gestion des absences • les processus liés aux RH et à l'administration de la paie : <ul style="list-style-type: none"> • l'administration de la paie; • l'inscription à des cursus ; • la gestion des compétences ; • les évaluations ; • l'examen des salaires ; • inscription des candidats à l'embauche ; • le traitement des paiements • facturation • demandes d'achats • la planification des ressources humaines/projets <p>Le Traitement impliquera :</p> <p>Produit (solution logicielle)</p> <p>Exécution par Unit4 ERP 8 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>Services</p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des Services supplémentaires, comme indiqué en détails dans la Description des Services Unit4 ou dans la Description de Services People Platform , selon ce qui est applicable ;</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 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 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"> • les demandes de déplacements ; • les demandes de remboursement de Frais ; • les Feuilles de Temps, • les Absences • les processus liés aux RH et à l'administration de la paie : • l'administration de la paie ; • les cursus ; • la gestion des compétences ; • les évaluations ; • l'examen des salaires ; • inscription des candidats à l'embauche ; • le traitement des paiements • la facturation • les Achats • la Planification de projets / de ressources <p>Le Traitement impliquera :</p> <p>Produit (solution logicielle)</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>Services</p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des Services supplémentaires , comme indiqué en détails dans la Description des Services ou dans la Description de Services People Platform selon ce qui est applicable;</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 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 peuvent inclure notamment :</p> <ul style="list-style-type: none"> • Enregistrement de Client / Fournisseur / Collaborateur; • Traitement des paiements; • Facturation; • Traitement des demandes de remboursement de Frais; • Demandes de déplacement; • Demandes d'Achats et Commandes; • Plannification des projets / ressources; • Processus liés aux RH et à l'administration de la paie:

	<ul style="list-style-type: none"> • Paie; • Traitement des feuilles de temps; • Gestion des Absences et congés • Inscription à des cursus; • Gestion des compétences; • Evaluations; • Revue des salaires; • Enregistrement des candidats; <p>Le Traitement impliquera:</p> <p>Produit (solution logicielle)</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>Services</p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des Services supplémentaires , comme indiqué en détails dans la Description des Services ou dans la Description de Services People Platform selon ce qui est applicable;</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 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"> • le recrutement d'étudiants potentiels ; • la réponse à des demandes de renseignements ; • les demandes de traitement ; • 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 ; • la planification et l'établissement des horaires pour le personnel de l'université. <p>Le Traitement impliquera :</p> <p>Produit (solution logicielle)</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>Services</p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des Services supplémentaires , comme indiqué en détails dans la Description de Services ou dans la Description de Services People Platform selon ce qui est applicable.</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 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&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"> • Budgétisation ; • Rapports financiers et autres ; • Distribution des rapports ; • Traitement des approbations ; • Planification des ressources humaines/projets. <p>Le traitement impliquera :</p> <p>Produit (solution logicielle)</p> <p>Exécution par Unit4 FP&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>Services</p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des Services supplémentaires , comme indiqué en détails dans la Description de Services ou dans la Description de Services People Platform selon ce qui est applicable.</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 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>

<p>Unit4 Talent Management</p>	<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"> • Gestion des ressources humaines; • Gestion de la performance du personnel; • Développement de talent; • Evaluation de candidat; • Acquisition de savoir -" Learning"; • Retours et appreciation; et • Statistiques sur le personnel et l'implication du personnel <p>Le traitement impliquera :</p> <p>Produit (solution logicielle)</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>Services</p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des Services supplémentaires , comme indiqué en détails dans la Description de Services ou dans la Description de Services People Platform selon ce qui est applicable.</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 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>
<p>Unit4 Assistance PSA Suite</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"> • Automatisation d'un département de services professionnels, y compris gestion des ressources humaines ou gestion financière ; • Gestion des temps d'activité quotidienne et gestion de projet • Saisie des temps et notes de frais avec justificatifs ; • Transformation d'opportunités en projets, budget et temps prévisionnels et planification de projets et de ressources • Suivi du temps d'activité et des notes de frais et émission de factures ; • Intégration de projets sur d'autres applications ; • Réalisation de la comptabilité par le biais d'intégration de données financières dans d'autres solutions. <p>Le Traitement impliquera:</p> <p>Produit (solution logicielle)</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>Services</p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des Services supplémentaires , comme indiqué en détails dans la Description de Services ou dans la Description de Services People Platform selon ce qui est applicable.</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 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"), Services de Localisation et Unit4 Apps</p>	<p>Les Données à Caractère Personnel seront saisies sur PPS, les Services de Localisation et/ou Unit4 Apps permettant les finalités indiquées pour les services telles que décrites dans la Description de Services PPS sur www.unit4.com/terms.</p> <p>En outre, les Données à Caractère Personnel seront saisies dans Wanda en utilisant le logiciel tiers choisi (par exemple Slack Integration ou autres Applications Microsoft (y compris Microsoft Teams)). Selon le Produit ou Service Unit4 utilisé par le Client, Wanda peut les aider à accomplir des tâches administratives pour les collaborateurs du Client. De telles tâches peuvent inclure :</p> <ul style="list-style-type: none"> • Les entrées saisies dans les feuilles de temps ; • Les entrées saisies dans les Frais • Les demandes de déplacement • Les demandes de bulletins de paie • Les entrées saisies pour les absences / congés • Les demandes de situation de compte • Les demandes d'achat. • • Le Traitement impliquera : • <p>Produit (solution logicielle)</p> <p>Exécution par Wandade 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>Services</p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des Services supplémentaires , comme indiqué en détails dans la Description de Services ou dans la Description de Services People Platform selon ce qui est applicable.</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance de unit4 PPS, des Services de Localisation et/ou Unit4 Apps 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>Accès aux Données à Caractère Personnel pour l'amélioration de produits par le biais du machine learning (intelligence artificielle) ou analyse de données.</p>
Unit4 Property Management	<p>Les Données à Caractère Personnel seront saisies dans Unit4 Property Management pour permettre au Client d'organiser et gérer les processus liés au fonctionnement opérationnel et la gestion et/ou administration de ses activités internes.</p> <p>Les Traitements peuvent inclure :</p> <ul style="list-style-type: none"> • Enregistrement du candidat/demandeur • Gestion locative • Processus de contrat de bail • Processus de l'association et/ou syndic de copropriété • Traitement des signatures électroniques • Prélèvement comprenant l'impression de facture • Traitement des paiements • Processus de relance • Modification de location. <p>Le Traitement impliquera:</p> <p>Produit (solution logicielle)</p> <p>Exécution par Unit4 Property 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>Services</p> <p>Transfert et conservation des Données à Caractère Personnel permettant d'offrir des Services supplémentaires , comme indiqué en détails dans la Description de Services ou dans la Description de Services People Platform selon ce qui est applicable.</p> <p>Accès aux Données à Caractère Personnel pour offrir une assistance et une maintenance du Produit Unit4 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
Unit4 SaaS (général)	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 d'Unit4 et les descriptions de Services Spécifiques à une Solution.	<p><u>Personnel</u></p> <p>L'équipe opérationnelle Cloud d'Unit4 a des collaborateurs dans les pays de l'UE (y compris sans y être limité en Pologne, Suède, Norvège, Pays-Bas, Espagne et Portugal), au Royaume-Uni, aux Etats-Unis d'Amérique, au Canada, en Malaisie et à Singapour. Lesdits membres du personnel du Sous-Traitant mettent en œuvre le SaaS d'Unit4.</p> <p><u>Biens et Infrastructure</u></p> <p>Unit4 utilise des services d'hébergement d'infrastructure tiers afin de le SaaS d'Unit4 et fait appel à d'autres systèmes logiciels pour la gestion et l'exécution. Voir Section 3.</p>
Unit4 Talent Management SaaS	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 applicable.	<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 le SaaS Talent Management d'Unit4.</p> <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 Section 3.</p>
Services d'Assistance	Le Sous-Traitant Traitera les Données à Caractère Personnel en lien avec les activités décrites au Contrat et plus	<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</p>

	spécifiquement dans les Conditions d'Assistance Unit4 .	Sous-Traitant fournissent les Services d'Assistance d'Unit4 (décrits dans les Conditions d'Assistance d'Unit4 au paragraphe B des Niveaux de Service). <u>Biens et Infrastructure</u> Unit4 utilise d'autres logiciels pour l'exploitation, la livraison et la gestion de ces services..
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.	<u>Personnel</u> 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. <u>Biens et Infrastructure</u> Unit4 utilise d'autres systèmes logiciels pour l'exploitation, la livraison et la gestion de ces services.
Services Professionnels Unit4 (si sous-traités à un partenaire en charge de la livraison)	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 la Section 3. Le Sous-Traitant conclura un accord écrit avec le(s) Sous-traitants ultérieurs, qui sera conforme avec la législation et les réglementations applicables et le Contrat. 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 Section 3.	Voir Section 3 du Bon de Commande applicable..
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 Section 3 ou le Bon de Commande applicable et toute stipulation supplémentaire dans les annexes et appendices aux Informations sur le Traitement de Données si cela est requis par le Fournisseur Tiers ou par ou le Droit Applicable.
People Platform Services ("PPS"), Services de Localisation et/ou Apps	Outre le SaaS d'Unit4, les Services PPS, les Services de Localisations et/ou Apps 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.	<u>Personnel</u> L'équipe opérationnelle Cloud d'Unit4, qui exploite la plateforme PPS, les Services de Localisation et/ou Apps compte du personnel dans les pays membres de l'UE (y compris mais sans y être limité en Pologne, Suède, Norvège, Pays-Bas, Espagne et Portugal), au Royaume Uni, aux Etats-Unis d'Amérique, Canada, Malaisie et Singapour. Lesdits membres du personnel du Sous-Traitant mettent en œuvre le service SaaS d'Unit4. <u>Biens et Infrastructure</u> Unit4 utilise ses propres services d'infrastructure et des services tiers (partagés) d'infrastructure pour fournir les services People Platform d'Unit4, les Services de Localisation et/ou Apps. Cela inclut les systèmes tiers (par exemple les applications de collaboration) sur lesquels Unit4 n'exerce aucun contrôle. Les PPS comprenant Wanda, les Services de Localisation et/ou Apps utilisent un certain nombre de produits et services Microsoft, comme suit : :Cognitive services: <ul style="list-style-type: none">○ LUIS Cognitive Service - compréhension de texte.○ Text Translator API – traduction de texte○ QnA Maker Cognitive service – fournit un service de questions / réponses● Bot framework connectors – fournit la connexion de Wanda aux réseaux sociaux "supportés ».● Traffic manager – utilisé pour la reprise d'activité après sinistre et basculement si la région principale est affectée● Web apps / web jobs – héberge des APIs web et des processus au long cours sur le web● Service bus – fournit de la communication interne dans l'écosystème Wanda● Storage accounts – utilise pour conserver l'état de conversation et les paramètres utilisateur● Cosmos DB –fournit du stockage

	<ul style="list-style-type: none"> • Fonctions – fournit des algorithmes logiciels pour les extensions • Event grid – fournit de la <i>communication</i> • API management – pour gérer les <i>APIs</i> • Service Plans – <i>Linux et plans de service dynamiques pour faire fonctionner le Service</i> • Storage accounts – <i>pour procéder au stockage</i> • Key vault – conserve des données confidentielles qui sont utilisées pour communiquer avec des services Microsoft et pour services internes • Redis cache – fournit des capacités de cache • Application Insights – supervision du système, y compris telemetrie et création d'incident • SQL server – fournit du stockage • Kubernetes – conteneur open source <p>De plus amples informations et détails sur les produits et les services Microsoft peuvent être trouvés ici: https://azure.microsoft.com/en-us/services/.</p> <p>En parallèle, les PPS, les Services de Localisation et /ou Apps Unit4 utilisent:</p> <p>Twilio – sendgrid – pour envoyer des messages électroniques</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 sur Microsoft Azure, et recouvre à la fois les Zones Géo-Politiques de l'Union Européenne et du Royaume-Uni (ci-dessus), selon la zone qui est allouée en fonction de la localisation du Client. Toutes les Données Clients, à l'exception du partage avec les sous-traitants ultérieurs sélectionnés dans la Section 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	Localisation du Client		Assistance principale fournie à partir des pays suivants (mais pouvant inclure d'autres pays de l'Union Européenne):
	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	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 ainsi que les Pays-Bas, l'Espagne et les autres sites tels que nécessaires pour les besoins de l'activité de Unit4.			
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), services de localisation et/ou Apps	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.			
	Service	Zone	Lieu où le Service Traite ou Conserve des Données	L'assistance est fournie principalement à partir de:
	Wanda	Toute zone	Principalement au sein de l'UE, mais cela peut être partout ailleurs globalement où il existe un centre de données Azure (par ex USA).	Pays de l'Union Européenne comprenant l'Irlande, la Pologne et l'Espagne ; les USA et autres services d'assistance globaux, selon la demande
	PPS, Services de Localisation et/ou Apps	Dépend du déploiement du Cloud	le Service est effectué et les données sont conservées dans les zones Géopolitiques sélectionnées	Comme ci-dessus pour SaaS
Services Professionnels Unit4 et la fonction « customer success » d'Unit4	Sujet	Les Services Professionnels et la fonction "customer success" sont fournis à partir de:		
	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 Informations sur le Traitement de Données, le point de contact suivant :

Le Responsable de Traitement peut adresser ses courriers au Sous-Traitant : par courrier (adressé au Global Data Protection 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 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.

SECTION 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 Section 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/ou 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.
- 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 (Chief Information Security Officer) et au Directeur Monde de la Protection des Données (Global Data Protection Officer) 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.
- 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 du SaaS Unit4 :

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 des bases de données sont chiffrées à l'aide d'une technologie de chiffrement des bases de données comme le Chiffrement Transparent des Bases de données.
- Les données et fichiers non-transactionnels seront sécurisés par *standard symmetric encryption (AES)*
- 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 de 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, ayant des instances distinctes de bases de données pour tous nos clients.

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 Données à Caractère Personnel 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.

Unit4 et les opérateurs de centres de données détiennent plusieurs certifications de sécurité dont les détails figurent dans la Description des Services applicable.

Éléments supplémentaires pour les services People Platform Services d'Unit4 (résumé)

Description des mesures de sécurité techniques et opérationnelles mises en oeuvre 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 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.

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.

SECTION 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 Section 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 la Section 2, paragraphe 5.	Fourniture d'infrastructure Cloud et Services Cloud
	Microsoft Dynamics	voir les indications ci-dessus à la Section 2, paragraphe 5.	Fourniture de Services Logiciels, en particulier Microsoft Dynamics (y compris certaines infrastructures cloud).
	Microsoft	voir les indications ci-dessus à la Section 2, paragraphe 5.	Fourniture d'outils logiciels et Office
	Conapto	voir les indications ci-dessus à la Section 2, paragraphe 5.	Fourniture d'infrastructures et de services Cloud
	Twilio - Sendgrid	USA (Privacy Policy)	Envoi de courriel (CCT de l'UE – voir Section 4)
Services Cloud d'Unit4 – Gestion des Talents	Microsoft Azure	Dublin, Irlande	Fourniture de solution - Suite
	LogDNA	USA (Privacy Policy)	Fourniture de solution – Suite (CCT de l'UE - voir Section 4)
	Mandrill	USA (Privacy Policy)	Fourniture de solution – Suite (CCT de l'UE - voir Section 4)
	Mixpanel	USA (Privacy Policy)	Fourniture de solution – Suite (CCT de l'UE - voir Section 4)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Fourniture de solution - Learn (SCORM uniquement) (CCT de l'UE - voir Section 4)
	Sentry	USA (Privacy Policy)	Fourniture de solution – Suite (CCT de l'UE - voir Section 4)
	Slack	USA (Privacy Policy)	Fourniture de solution – Perform (CCT de l'UE - voir Section 4)
	Wistia	USA (Privacy Policy)	Fourniture de solution – Learn (CCT de l'UE - voir Section 4)
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'Section 1, paragraphe 5 et tel que décrit par Microsoft ici: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located .	Fourniture d'infrastructure et services de plateforme Cloud (tel que décrit ci-dessus) à la section 2
	Twilio - Sendgrid	USA (Privacy Policy)	Envoi de courriels (CCT de l'UE – voir Section 4)

SECTION 4 – CLAUSES CONTRACTUELLES TYPES DE L'UE

CLAUSES CONTRACTUELLES TYPES ("CCT")

Responsable de Traitement vers Sous-traitant

Unit4 est le Sous-Traitant/importateur de données

Le Client est le Responsable de Traitement/exportateur de données

En ce qui concerne les relations entre les Parties, le Module Deux (transfert responsable de traitement vers le sous-traitant) des CCT est applicable.

Les présentes CCT ne s'appliquent que lorsqu'il y a un transfert par le Responsable de Traitement de Données à caractère personnel à partir de l'EEE vers le Sous-Traitant à l'extérieur de l'EEE, également dénommé pays tiers, et lorsque aucune décision d'adéquation ne s'applique.

SECTION I

Clause 1

Finalités et champ d'application

a) Les présentes clauses contractuelles types visent à garantir le respect des exigences du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) [\(1\)](#) en cas de transfert de données à caractère personnel vers un pays tiers.

b) Les parties:

i) la ou les personnes physiques ou morales, la ou les autorités publiques, la ou les agences ou autre(s) organisme(s) (ci-après la ou les «entités») qui transfèrent les données à caractère personnel, mentionnés à l'annexe I.A. (ci-après l'«exportateur de données»), et

ii) la ou les entités d'un pays tiers qui reçoivent les données à caractère personnel de l'exportateur de données, directement ou indirectement par l'intermédiaire d'une autre entité également partie aux présentes clauses, mentionnées à l'annexe I.A. (ci-après l'«importateur de données»)

sont convenues des présentes clauses contractuelles types (ci-après les «clauses»).

c) Les présentes clauses s'appliquent au transfert de données à caractère personnel précisé à l'annexe I.B.

d) L'appendice aux présentes clauses, qui contient les annexes qui y sont mentionnées, fait partie intégrante des présentes clauses.

Clause 2

Effet et invariabilité des clauses

a) Les présentes clauses établissent des garanties appropriées, notamment des droits opposables pour la personne concernée et des voies de droit effectives, en vertu de l'article 46, paragraphe 1, et de l'article 46, paragraphe 2, point c), du règlement (UE) 2016/679 et, en ce qui concerne les transferts de données de responsables du traitement à sous-traitants et/ou de sous-traitants à sous-traitants, des clauses contractuelles types en vertu de l'article 28, paragraphe 7, du règlement (UE) 2016/679, à condition qu'elles ne soient pas modifiées, sauf pour sélectionner le ou les modules appropriés ou pour ajouter ou mettre à jour des informations dans l'appendice. Cela n'empêche pas les parties d'inclure les clauses contractuelles types prévues dans les présentes clauses dans un contrat plus large et/ou d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les présentes clauses et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

b) Les présentes clauses sont sans préjudice des obligations auxquelles l'exportateur de données est soumis en vertu du règlement (UE) 2016/679.

Clause 3

Tiers bénéficiaires

a) Les personnes concernées peuvent invoquer et faire appliquer les présentes clauses, en tant que tiers bénéficiaires, contre l'exportateur et/ou l'importateur de données, avec les exceptions suivantes:

i) clause 1, clause 2, clause 3, clause 6, clause 7;

ii) clause 8 — module 1: clause 8.5, paragraphe e), et clause 8.9, paragraphe b); module 2: clause 8.1, paragraphe b), clause 8.9, paragraphes a), c), d) et e); module 3: clause 8.1, paragraphes a), c) et d) et clause 8.9, paragraphes a), c), d), e), f) et g); module 4: clause 8.1, paragraphe b), et clause 8.3, paragraphe b);

iii) clause 9 — module 2: clause 9, paragraphes a), c), d) et e); module 3: clause 9, paragraphes a) c), d) et e);

iv) clause 12 — module 1: clause 12, paragraphes a) et d); modules 2 et 3: clause 12, paragraphes a), d) et f);

v) clause 13;

vi) clause 15.1, paragraphes c), d) et e);

vii) clause 16, paragraphe e);

viii) clause 18 — modules 1, 2 et 3: clause 18, paragraphes a) et b); module 4: clause 18.

b) Le paragraphe a) est sans préjudice des droits des personnes concernées au titre du règlement (UE) 2016/679.

Clause 4

Interprétation

a) Lorsque les présentes clauses utilisent des termes définis dans le règlement (UE) 2016/679, ceux-ci ont la même signification que dans ledit règlement.

b) Les présentes clauses sont lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679.

c) Les présentes clauses ne sont pas interprétées dans un sens contraire aux droits et obligations prévus dans le règlement (UE) 2016/679.

Clause 5

Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes entre les parties existant au moment où les présentes clauses sont convenues, ou souscrites par la suite, les présentes clauses prévalent.

Clause 6

Description du ou des transferts

Les détails du ou des transferts, en particulier les catégories de données à caractère personnel qui sont transférées et la ou les finalités pour lesquelles elles le sont, sont précisés à l'annexe I.B.

Clause 7 — Facultative

Clause d'adhésion

- a) Une entité qui n'est pas partie aux présentes clauses peut, avec l'accord des parties, y adhérer à tout moment, soit en tant qu'exportateur de données soit en tant qu'importateur de données, en remplissant l'appendice et en signant l'annexe I.A.
- b) Une fois l'appendice rempli et l'annexe I.A. signée, l'entité adhérente devient partie aux présentes clauses et a les droits et obligations d'un exportateur de données ou d'un importateur de données selon sa désignation dans l'annexe I.A.
- c) L'entité adhérente n'a aucun droit ni obligation découlant des présentes clauses pour la période antérieure à son adhésion à celles-ci.

SECTION II — OBLIGATIONS DES PARTIES

Clause 8

Garanties en matière de protection des données

L'exportateur de données garantit qu'il a entrepris des démarches raisonnables pour s'assurer que l'importateur de données est à même, par la mise en œuvre de mesures techniques et organisationnelles appropriées, de satisfaire aux obligations qui lui incombent en vertu des présentes clauses.

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

8.1. Instructions

- a) L'importateur de données ne traite les données à caractère personnel que sur instructions documentées de l'exportateur de données. L'exportateur de données peut donner ces instructions pendant toute la durée du contrat.
- b) S'il n'est pas en mesure de suivre ces instructions, l'importateur de données en informe immédiatement l'exportateur de données.

8.2. Limitation des finalités

L'importateur de données traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du transfert, telles que précisées à l'annexe I.B, sauf en cas d'instructions supplémentaires de l'exportateur de données.

8.3. Transparence

Sur demande, l'exportateur de données met gratuitement à la disposition de la personne concernée une copie des présentes clauses, notamment de l'appendice tel que rempli par les parties. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les mesures décrites à l'annexe II et les données à caractère personnel, l'exportateur de données peut occulter une partie du texte de l'appendice aux présentes clauses avant d'en communiquer une copie, mais fournit un résumé valable s'il serait autrement impossible, pour la personne concernée, d'en comprendre le contenu ou d'exercer ses droits. Les parties fournissent à la personne concernée, à la demande de celle-ci, les motifs des occultations, dans la mesure du possible sans révéler les informations occultées. Cette clause est sans préjudice des obligations qui incombent à l'exportateur de données en vertu des articles 13 et 14 du règlement (UE) 2016/679.

8.4. Exactitude

Si l'importateur de données se rend compte que les données à caractère personnel qu'il a reçues sont inexactes, ou sont obsolètes, il en informe l'exportateur de données dans les meilleurs délais. Dans ce cas, l'importateur de données coopère avec l'exportateur de données pour effacer ou rectifier les données.

8.5. Durée du traitement et effacement ou restitution des données

Le traitement par l'importateur de données n'a lieu que pendant la durée précisée à l'annexe I.B. Au terme de la prestation des services de traitement, l'importateur de données, à la convenance de l'exportateur de données, efface toutes les données à caractère personnel traitées pour le compte de ce dernier et lui en apporte la preuve, ou lui restitue toutes les données à caractère personnel traitées pour son compte et efface les copies existantes. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données à caractère personnel que dans la mesure où et aussi longtemps que cette législation locale l'exige. Ceci est sans préjudice de la clause 14, en particulier de l'obligation imposée à l'importateur de données par la clause 14, paragraphe e), d'informer l'exportateur de données, pendant toute la durée du contrat, s'il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences de la clause 14, paragraphe a).

8.6. Sécurité du traitement

- a) L'importateur de données et, durant la transmission, l'exportateur de données mettent en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données, notamment pour les protéger d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à ces données (ci-après la «violation de données à caractère personnel»). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et de la ou des finalités du traitement ainsi que des risques inhérents au traitement pour les personnes concernées. Les parties envisagent en particulier de recourir au chiffrement ou à la pseudonymisation, notamment pendant la transmission, lorsque la finalité du traitement peut être atteinte de cette manière. En cas de pseudonymisation, les informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée précise restent, dans la mesure du possible, sous le contrôle exclusif de l'exportateur de données. Pour s'acquitter des obligations qui lui incombent en vertu du présent paragraphe, l'importateur de données met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe II. Il procède à des contrôles réguliers pour s'assurer que ces mesures continuent d'offrir le niveau de sécurité approprié.
- b) L'importateur de données ne donne l'accès aux données à caractère personnel aux membres de son personnel que dans la mesure strictement nécessaire à la mise en œuvre, à la gestion et au suivi du contrat. Il veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.
- c) En cas de violation de données à caractère personnel concernant des données à caractère personnel traitées par l'importateur de données au titre des présentes clauses, ce dernier prend des mesures appropriées pour remédier à la violation, y compris des mesures visant à en atténuer les effets négatifs. L'importateur de données informe également l'exportateur de données de cette violation dans les meilleurs délais après en avoir eu connaissance. Cette notification contient les coordonnées d'un point de contact auprès duquel il est possible d'obtenir plus d'informations, ainsi qu'une description de la nature de la violation (y compris, si possible, les catégories et le nombre approximatif de personnes concernées et d'enregistrements de données à caractère personnel concernés), de ses conséquences probables et des mesures prises ou proposées pour y remédier, y compris, le cas échéant, des mesures visant à en atténuer les effets négatifs potentiels. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et les autres informations sont fournies par la suite, dans les meilleurs délais, à mesure qu'elles deviennent disponibles.

d) L'importateur de données coopère avec l'exportateur de données et l'aide afin de lui permettre de respecter les obligations qui lui incombent en vertu du règlement (UE) 2016/679, notamment celle d'informer l'autorité de contrôle compétente et les personnes concernées, compte tenu de la nature du traitement et des informations à la disposition de l'importateur de données.

8.7. Données sensibles

Lorsque le transfert concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne, ou des données relatives à des condamnations pénales et à des infractions (ci-après les «données sensibles»), l'importateur de données applique les restrictions particulières et/ou les garanties supplémentaires décrites à l'annexe I.B.

8.8. Transferts ultérieurs

L'importateur de données ne divulgue les données à caractère personnel à un tiers que sur instructions documentées de l'exportateur de données. En outre, les données ne peuvent être divulguées à un tiers situé en dehors de l'Union européenne (4) (dans le même pays que l'importateur de données ou dans un autre pays tiers, ci-après «transfert ultérieur»), que si le tiers est lié par les présentes clauses ou accepte de l'être, en vertu du module approprié, ou si:

- i) le transfert ultérieur est effectué vers un pays bénéficiant d'une décision d'adéquation en vertu de l'article 45 du règlement (UE) 2016/679 qui couvre le transfert ultérieur;
- ii) le tiers offre d'une autre manière des garanties appropriées conformément aux articles 46 ou 47 du règlement (UE) 2016/679 en ce qui concerne le traitement en question;
- iii) le transfert ultérieur est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice dans le contexte de procédures administratives, réglementaires ou judiciaires spécifiques; ou
- iv) le transfert ultérieur est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Tout transfert ultérieur est soumis au respect, par l'importateur de données, de toutes les autres garanties au titre des présentes clauses, en particulier de la limitation des finalités.

8.9. Documentation et conformité

- a) L'importateur de données traite rapidement et de manière appropriée les demandes de renseignements de l'exportateur de données concernant le traitement au titre des présentes clauses.
- b) Les parties sont en mesure de démontrer le respect des présentes clauses. En particulier, l'importateur de données conserve une trace documentaire appropriée des activités de traitement menées pour le compte de l'exportateur de données.
- c) L'importateur de données met à la disposition de l'exportateur de données toutes les informations nécessaires pour démontrer le respect des obligations prévues par les présentes clauses et, à la demande de l'exportateur de données, pour permettre la réalisation d'audits des activités de traitement couvertes par les présentes clauses, et contribuer à ces audits, à intervalles raisonnables ou s'il existe des indications de non-respect. Lorsqu'il décide d'un examen ou d'un audit, l'exportateur de données peut tenir compte des certifications pertinentes détenues par l'importateur de données.
- d) L'exportateur de données peut choisir de procéder à l'audit lui-même ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques de l'importateur de données et sont, le cas échéant, effectués avec un préavis raisonnable.
- e) Les parties mettent à la disposition de l'autorité de contrôle compétente, à la demande de celle-ci, les informations mentionnées aux paragraphes b) et c), y compris les résultats de tout audit.

Clause 9

Recours à des sous-traitants ultérieurs

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

- a) **AUTORISATION ÉCRITE GÉNÉRALE** — L'importateur de données a l'autorisation générale de l'exportateur de données de recruter un ou plusieurs sous-traitants ultérieurs à partir d'une liste arrêtée d'un commun accord. L'importateur de données informe expressément par écrit l'exportateur de données de tout changement concernant l'ajout ou le remplacement de sous-traitants ultérieurs qu'il est prévu d'apporter à cette liste au moins 30 jours à l'avance, donnant ainsi à l'exportateur de données suffisamment de temps pour émettre des objections à l'encontre de ces changements avant le recrutement du ou des sous-traitants ultérieurs. L'importateur de données fournit à l'exportateur de données les informations nécessaires pour permettre à ce dernier d'exercer son droit d'émettre des objections.
- b) Lorsque l'importateur de données recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte de l'exportateur de données), il le fait au moyen d'un contrat écrit qui prévoit, en substance, les mêmes obligations en matière de protection des données que celles qui lient l'importateur de données au titre des présentes clauses, notamment en ce qui concerne les droits du tiers bénéficiaire pour les personnes concernées (5). Les parties conviennent qu'en respectant la présente clause, l'importateur de données satisfait aux obligations qui lui incombent en vertu de la clause 8.8. L'importateur de données veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses.
- c) L'importateur de données fournit à l'exportateur de données, à la demande de celui-ci, une copie du contrat avec le sous-traitant ultérieur et de ses éventuelles modifications ultérieures. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les données à caractère personnel, l'importateur de données peut occulter une partie du texte du contrat avant d'en communiquer une copie.
- d) L'importateur de données reste pleinement responsable à l'égard de l'exportateur de données de l'exécution des obligations qui incombent au sous-traitant ultérieur en vertu du contrat qu'il a conclu avec lui. L'importateur de données notifie à l'exportateur de données tout manquement du sous-traitant ultérieur aux obligations qui lui incombent en vertu dudit contrat.
- e) L'importateur de données convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire en vertu de laquelle, dans les cas où l'importateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'exportateur de données a le droit de résilier le contrat du sous-traitant ultérieur et de donner instruction à ce dernier d'effacer ou de restituer les données à caractère personnel.

Clause 10

Droits des personnes concernées

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

- a) L'importateur de données informe rapidement l'exportateur de données de toute demande reçue d'une personne concernée. Il ne répond pas lui-même à cette demande, à moins d'y avoir été autorisé par l'exportateur de données.
- b) L'importateur de données aide l'exportateur de données à s'acquitter de son obligation de répondre aux demandes de personnes concernées désireuses d'exercer leurs droits en vertu du règlement (UE) 2016/679. À cet égard, les parties indiquent à l'annexe II les mesures techniques et organisationnelles appropriées, compte tenu de la nature du traitement, au moyen desquelles l'aide sera fournie, ainsi que la portée et l'étendue de l'aide requise.

c) Lorsqu'il s'acquiesce des obligations qui lui incombent en vertu des paragraphes a) et b), l'importateur de données se conforme aux instructions de l'exportateur de données.

Clause 11

Voies de recours

a) L'importateur de données informe les personnes concernées, sous une forme transparente et aisément accessible, au moyen d'une notification individuelle ou sur son site web, d'un point de contact autorisé à traiter les réclamations. Il traite sans délai toute réclamation reçue d'une personne concernée.

[OPTION: L'importateur de données convient que les personnes concernées peuvent également introduire, sans frais, une réclamation auprès d'un organe de règlement des litiges indépendant ⁽¹⁾. Il informe les personnes concernées, de la manière indiquée au paragraphe a), de ce mécanisme de recours et du fait qu'elles ne sont pas tenues d'y recourir ni de respecter une hiérarchie dans les recours.]

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

Clause 12

Responsabilité

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

a) Chaque partie est responsable envers la ou les autres parties des dommages qu'elle cause à l'autre ou aux autres parties du fait d'un manquement aux présentes clauses.

b) L'importateur de données est responsable à l'égard de la personne concernée, et la personne concernée a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par l'importateur de données ou son sous-traitant ultérieur du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses.

c) Nonobstant le paragraphe b), l'exportateur de données est responsable à l'égard de la personne concernée et celle-ci a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par l'exportateur de données ou l'importateur de données (ou son sous-traitant ultérieur) du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses. Ceci est sans préjudice de la responsabilité de l'exportateur de données et, si l'exportateur de données est un sous-traitant agissant pour le compte d'un responsable du traitement, de la responsabilité de ce dernier au titre du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725, selon le cas.

d) Les parties conviennent que, si l'exportateur de données est reconnu responsable, en vertu du paragraphe c), du dommage causé par l'importateur de données (ou son sous-traitant ultérieur), il a le droit de réclamer auprès de l'importateur de données la part de la réparation correspondant à la responsabilité de celui-ci dans le dommage.

e) Lorsque plusieurs parties sont responsables d'un dommage causé à la personne concernée du fait d'une violation des présentes clauses, toutes les parties responsables le sont conjointement et solidairement et la personne concernée a le droit d'intenter une action en justice contre n'importe laquelle de ces parties.

f) Les parties conviennent que, si la responsabilité d'une d'entre elles est reconnue en vertu du paragraphe e), celle-ci a le droit de réclamer auprès de l'autre ou des autres parties la part de la réparation correspondant à sa/leur responsabilité dans le dommage.

g) L'importateur de données ne peut invoquer le comportement d'un sous-traitant ultérieur pour échapper à sa propre responsabilité.

Clause 13

Contrôle

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

a) [Si l'exportateur de données est établi dans un État membre de l'Union:] L'autorité de contrôle chargée de garantir le respect, par l'exportateur de données, du règlement (UE) 2016/679 en ce qui concerne le transfert de données, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité de contrôle compétente.

[Si l'exportateur de données n'est pas établi dans un État membre de l'Union, mais relève du champ d'application territorial du règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2, et a désigné un représentant en vertu de l'article 27, paragraphe 1, dudit règlement:] L'autorité de contrôle de l'État membre dans lequel le représentant au sens de l'article 27, paragraphe 1, du règlement (UE) 2016/679 est établi, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité de contrôle compétente.

[Si l'exportateur de données n'est pas établi dans un État membre de l'Union, mais relève du champ d'application territorial du règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2 sans toutefois avoir à désigner un représentant en vertu de l'article 27, paragraphe 2, du règlement (UE) 2016/679:] L'autorité de contrôle d'un des États membres dans lesquels se trouvent les personnes concernées dont les données à caractère personnel sont transférées au titre des présentes clauses en lien avec l'offre de biens ou de services ou dont le comportement fait l'objet d'un suivi, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité compétente.

b) L'importateur de données accepte de se soumettre à la juridiction de l'autorité de contrôle compétente et de coopérer avec elle dans le cadre de toute procédure visant à garantir le respect des présentes clauses. En particulier, l'importateur de données accepte de répondre aux demandes de renseignements, de se soumettre à des audits et de se conformer aux mesures adoptées par l'autorité de contrôle, notamment aux mesures correctrices et compensatoires. Il confirme par écrit à l'autorité de contrôle que les mesures nécessaires ont été prises.

SECTION III — LÉGISLATIONS LOCALES ET OBLIGATIONS EN CAS D'ACCÈS DES AUTORITÉS PUBLIQUES

Clause 14

Législations et pratiques locales ayant une incidence sur le respect des clauses

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

a) Les parties garantissent qu'elles n'ont aucune raison de croire que la législation et les pratiques du pays tiers de destination applicables au traitement des données à caractère personnel par l'importateur de données, notamment les exigences en matière de divulgation de données à caractère personnel ou les mesures autorisant l'accès des autorités publiques à ces données, empêchent l'importateur de données de s'acquiescer des obligations qui lui incombent en vertu des présentes clauses. Cette disposition repose sur l'idée que les législations et les pratiques qui respectent l'essence des libertés et droits fondamentaux et qui n'excèdent pas ce qui est nécessaire et proportionné dans une société démocratique pour préserver un des objectifs énumérés à l'article 23, paragraphe 1, du règlement (UE) 2016/679 ne sont pas en contradiction avec les présentes clauses.

b) Les parties déclarent qu'en fournissant la garantie mentionnée au paragraphe a), elles ont dûment tenu compte, en particulier, des éléments suivants:

i) des circonstances particulières du transfert, parmi lesquelles la longueur de la chaîne de traitement, le nombre d'acteurs concernés et les canaux de transmission utilisés; les transferts ultérieurs prévus; le type de destinataire; la finalité du traitement; les catégories et le format des données à caractère personnel transférées; le secteur économique dans lequel le transfert a lieu et le lieu de stockage des données transférées;

- ii) des législations et des pratiques du pays tiers de destination – notamment celles qui exigent la divulgation de données aux autorités publiques ou qui autorisent l'accès de ces dernières aux données – pertinentes au regard des circonstances particulières du transfert, ainsi que des limitations et des garanties applicables ⁽¹²⁾;
 - iii) de toute garantie contractuelle, technique ou organisationnelle pertinente mise en place pour compléter les garanties prévues par les présentes clauses, y compris les mesures appliquées pendant la transmission et au traitement des données à caractère personnel dans le pays de destination.
- c) L'importateur de données garantit que, lors de l'évaluation au titre du paragraphe b), il a déployé tous les efforts possibles pour fournir des informations pertinentes à l'exportateur de données et convient qu'il continuera à coopérer avec ce dernier pour garantir le respect des présentes clauses.
- d) Les parties conviennent de conserver une trace documentaire de l'évaluation au titre du paragraphe b) et de mettre cette évaluation à la disposition de l'autorité de contrôle compétente si celle-ci en fait la demande.
- e) L'importateur de données accepte d'informer sans délai l'exportateur de données si, après avoir souscrit aux présentes clauses et pendant la durée du contrat, il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences du paragraphe a), notamment à la suite d'une modification de la législation du pays tiers ou d'une mesure (telle qu'une demande de divulgation) indiquant une application pratique de cette législation qui n'est pas conforme aux exigences du paragraphe a). [Pour le module 3: l'exportateur de données transmet la notification au responsable du traitement.]
- f) À la suite d'une notification au titre du paragraphe e), ou si l'exportateur de données a d'autres raisons de croire que l'importateur de données ne peut plus s'acquitter des obligations qui lui incombent en vertu des présentes clauses, l'exportateur de données définit sans délai les mesures appropriées (par exemple des mesures techniques ou organisationnelles visant à garantir la sécurité et la confidentialité) qu'il doit adopter et/ou qui doivent être adoptées par l'importateur de données pour remédier à la situation, [pour le module 3: si nécessaire en concertation avec le responsable du traitement]. L'exportateur de données suspend le transfert de données s'il estime qu'aucune garantie appropriée ne peut être fournie pour ce transfert ou si [pour le module 3: le responsable du traitement ou] l'autorité de contrôle compétente lui en donne [pour le module 3: donne] l'instruction. Dans ce cas, l'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement. Lorsque le contrat est résilié en vertu de la présente clause, la clause 16, paragraphes d) et e), s'applique.

Clause 15

Obligations de l'importateur de données en cas d'accès des autorités publiques

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

15.1. Notification

- a) L'importateur de données convient d'informer sans délai l'exportateur de données et, si possible, la personne concernée (si nécessaire avec l'aide de l'exportateur de données):
- i) s'il reçoit une demande juridiquement contraignante d'une autorité publique, y compris judiciaire, en vertu de la législation du pays de destination en vue de la divulgation de données à caractère personnel transférées au titre des présentes clauses; cette notification comprend des informations sur les données à caractère personnel demandées, l'autorité requérante, la base juridique de la demande et la réponse fournie; ou
 - ii) s'il a connaissance d'un quelconque accès direct des autorités publiques aux données à caractère personnel transférées au titre des présentes clauses en vertu de la législation du pays de destination; cette notification comprend toutes les informations dont l'importateur de données dispose.
- [Pour le module 3: L'exportateur de données transmet la notification au responsable du traitement.]
- b) Si la législation du pays de destination interdit à l'importateur de données d'informer l'exportateur de données et/ou la personne concernée, l'importateur de données convient de tout mettre en œuvre pour obtenir une levée de cette interdiction, en vue de communiquer autant d'informations que possible, dans les meilleurs délais. L'importateur de données accepte de garder une trace documentaire des efforts qu'il a déployés afin de pouvoir en apporter la preuve à l'exportateur de données, si celui-ci lui en fait la demande.
- c) Lorsque la législation du pays de destination le permet, l'importateur de données accepte de fournir à l'exportateur de données, à intervalles réguliers pendant la durée du contrat, autant d'informations utiles que possible sur les demandes reçues (notamment le nombre de demandes, le type de données demandées, la ou les autorités requérantes, la contestation ou non des demandes et l'issue de ces contestations, etc.). [Pour le module 3: L'exportateur de données transmet les informations au responsable du traitement.]
- d) L'importateur de données accepte de conserver les informations mentionnées aux paragraphes a) à c) pendant la durée du contrat et de les mettre à la disposition de l'autorité de contrôle compétente si celle-ci lui en fait la demande.
- e) Les paragraphes a) à c) sont sans préjudice de l'obligation incombant à l'importateur de données, en vertu de la clause 14, paragraphe e), et de la clause 16, d'informer sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses.

15.2. Contrôle de la légalité et minimisation des données

- a) L'importateur de données accepte de contrôler la légalité de la demande de divulgation, en particulier de vérifier si elle s'inscrit dans les limites des pouvoirs conférés à l'autorité publique requérante, et de la contester si, après une évaluation minutieuse, il conclut qu'il existe des motifs raisonnables de considérer qu'elle est illégale en vertu de la législation du pays de destination, des obligations applicables en vertu du droit international et des principes de courtoisie internationale. L'importateur de données exerce les possibilités d'appel ultérieures dans les mêmes conditions. Lorsqu'il conteste une demande, l'importateur de données demande des mesures provisoires visant à suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente se prononce sur son bien-fondé. Il ne divulgue pas les données à caractère personnel demandées tant qu'il n'est pas obligé de le faire en vertu des règles de procédure applicables. Ces exigences sont sans préjudice des obligations incombant à l'importateur de données en vertu de la clause 14, paragraphe e).
- b) L'importateur de données accepte de garder une trace documentaire de son évaluation juridique ainsi que de toute contestation de la demande de divulgation et, dans la mesure où la législation du pays de destination le permet, de mettre les documents concernés à la disposition de l'exportateur de données. Il les met également à la disposition de l'autorité de contrôle compétente si celle-ci lui en fait la demande. [Pour le module 3: L'exportateur de données met l'évaluation à la disposition du responsable du traitement.]
- c) L'importateur de données accepte de fournir le minimum d'informations autorisé lorsqu'il répond à une demande de divulgation, sur la base d'une interprétation raisonnable de la demande.

SECTION IV — DISPOSITIONS FINALES

Clause 16

Non-respect des clauses et résiliation

- a) L'importateur de données informe sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses, quelle qu'en soit la raison.

b) Dans le cas où l'importateur de données enfreint les présentes clauses ou n'est pas en mesure de les respecter, l'exportateur de données suspend le transfert de données à caractère personnel à l'importateur de données jusqu'à ce que le respect des présentes clauses soit à nouveau garanti ou que le contrat soit résilié. Ceci est sans préjudice de la clause 14, paragraphe f).

c) L'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses, lorsque:

- i) l'exportateur de données a suspendu le transfert de données à caractère personnel à l'importateur de données en vertu du paragraphe b) et que le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension;
- ii) l'importateur de données enfreint gravement ou de manière persistante les présentes clauses; ou
- iii) l'importateur de données ne se conforme pas à une décision contraignante d'une juridiction ou d'une autorité de contrôle compétente concernant les obligations qui lui incombent au titre des présentes clauses.

Dans ces cas, il informe l'autorité de contrôle compétente [pour le module 3: et le responsable du traitement] de ce non-respect. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement.

d) [Pour les modules 1, 2 et 3: Les données à caractère personnel qui ont été transférées avant la résiliation du contrat au titre du paragraphe c) sont immédiatement restituées à l'exportateur de données ou effacées dans leur intégralité, à la convenance de celui-ci. Il en va de même pour toute copie des données.] [Pour le module 4: Les données à caractère personnel collectées par l'exportateur de données dans l'Union qui ont été transférées avant la résiliation du contrat au titre du paragraphe c), ainsi que toute copie de celles-ci, sont immédiatement effacées dans leur intégralité.] L'importateur de données apporte la preuve de l'effacement des données à l'exportateur de données. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel transférées, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données que dans la mesure où et aussi longtemps que cette législation locale l'exige.

e) Chaque partie peut révoquer son consentement à être liée par les présentes clauses i) si la Commission européenne adopte une décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 qui couvre le transfert de données à caractère personnel auquel les présentes clauses s'appliquent; ou ii) si le règlement (UE) 2016/679 est intégré dans le cadre juridique du pays vers lequel les données à caractère personnel sont transférées. Ceci est sans préjudice des autres obligations qui s'appliquent au traitement en question en vertu du règlement (UE) 2016/679.

Clause 17

Droit applicable

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

Les présentes clauses sont régies par le droit d'un des États membres de l'Union européenne, pour autant que ce droit reconnaisse des droits au tiers bénéficiaire. Les parties conviennent qu'il s'agit du droit applicable stipulé dans le Contrat.

Clause 18

Élection de for et juridiction

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

a) Tout litige survenant du fait des présentes clauses est tranché par les juridictions d'un État membre de l'Union européenne.

b) Les parties conviennent qu'il s'agit des juridictions compétentes selon le droit applicable stipulé dans le Contrat.

c) La personne concernée peut également poursuivre l'exportateur et/ou l'importateur de données devant les juridictions de l'État membre dans lequel elle a sa résidence habituelle.

d) Les parties acceptent de se soumettre à la compétence de ces juridictions.

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

⁽²⁾ Cela nécessite de rendre les données anonymes de telle manière que la personne ne soit plus identifiable par qui que ce soit, conformément au considérant 26 du règlement (UE) 2016/679, et que ce processus soit irréversible.

⁽³⁾ L'accord sur l'Espace économique européen (accord EEE) prévoit l'extension du marché intérieur de l'Union européenne aux trois pays de l'EEE que sont l'Islande, le Liechtenstein et la Norvège. La législation de l'Union en matière de protection des données, notamment le règlement (UE) 2016/679, est couverte par l'accord EEE et a été intégrée dans l'annexe XI de celui-ci. Dès lors, une divulgation par l'importateur de données à un tiers situé dans l'EEE ne peut être qualifiée de transfert ultérieur aux fins des présentes clauses.

⁽⁴⁾ L'accord sur l'Espace économique européen (accord EEE) prévoit l'extension du marché intérieur de l'Union européenne aux trois pays de l'EEE que sont l'Islande, le Liechtenstein et la Norvège. La législation de l'Union en matière de protection des données, notamment le règlement (UE) 2016/679, est couverte par l'accord EEE et a été intégrée dans l'annexe XI de celui-ci. Dès lors, une divulgation par l'importateur de données à un tiers situé dans l'EEE ne peut être qualifiée de transfert ultérieur aux fins des présentes clauses.

⁽⁵⁾ Voir l'article 28, paragraphe 4, du règlement (UE) 2016/679 et, lorsque le responsable du traitement est une institution ou un organe de l'Union, l'article 29, paragraphe 4, du règlement (UE) 2018/1725.

⁽⁶⁾ L'accord sur l'Espace économique européen (accord EEE) prévoit l'extension du marché intérieur de l'Union européenne aux trois pays de l'EEE que sont l'Islande, le Liechtenstein et la Norvège. La législation de l'Union en matière de protection des données, notamment le règlement (UE) 2016/679, est couverte par l'accord EEE et a été intégrée dans l'annexe XI de celui-ci. Dès lors, une divulgation par l'importateur de données à un tiers situé dans l'EEE ne peut être qualifiée de transfert ultérieur aux fins des présentes clauses.

⁽⁷⁾ Il s'agit notamment de savoir si le transfert et le traitement ultérieur portent sur des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques ou des données biométriques aux fins

d'identifier une personne physique de manière unique, des données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne, ou des données relatives à des condamnations pénales ou à des infractions.

⁽⁸⁾ Cette exigence peut être satisfaite par l'adhésion du sous-traitant ultérieur aux présentes clauses en vertu du module approprié, conformément à la clause 7.

⁽⁹⁾ Cette exigence peut être satisfaite par l'adhésion du sous-traitant ultérieur aux présentes clauses en vertu du module approprié, conformément à la clause 7.

⁽¹⁰⁾ Ce délai peut être prolongé de deux mois maximum, dans la mesure nécessaire compte tenu de la complexité des demandes et de leur nombre. L'importateur de données informe dûment et rapidement la personne concernée de cette prolongation.

⁽¹¹⁾ L'importateur de données ne peut proposer un règlement des litiges indépendant par une instance d'arbitrage que s'il est établi dans un pays qui a ratifié la convention de New York pour la reconnaissance et l'exécution des sentences arbitrales étrangères.

⁽¹²⁾ En ce qui concerne l'incidence de ces législations et pratiques sur le respect des présentes clauses, différents éléments peuvent être considérés comme faisant partie d'une évaluation globale. Ces éléments peuvent inclure une expérience concrète, documentée et pertinente de cas antérieurs de demandes de divulgation émanant d'autorités publiques, ou l'absence de telles demandes, couvrant un laps de temps suffisamment représentatif. Il peut s'agir de registres internes ou d'autres documents établis de manière continue conformément au principe de diligence raisonnable et certifiés à un niveau hiérarchique élevé, pour autant que ces informations puissent être partagées légalement avec des tiers. Lorsque cette expérience pratique est invoquée pour conclure que l'importateur de données ne sera pas empêché de respecter les présentes clauses, il y a lieu de l'étayer par d'autres éléments pertinents et objectifs, et il appartient aux parties d'examiner avec soin si ces éléments, pris dans leur ensemble, ont un poids suffisant, du point de vue de leur fiabilité et de leur représentativité, pour soutenir cette conclusion. En particulier, les parties doivent s'assurer que leur expérience pratique est corroborée et non contredite par des informations fiables accessibles au public ou disponibles d'une autre manière sur l'existence ou l'absence de demandes dans le même secteur et/ou sur l'application pratique du droit, comme la jurisprudence et les rapports d'organes de contrôle indépendants.

APPENDICE

NOTE EXPLICATIVE:

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

ANNEXE I

A. LISTE DES PARTIES

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

Exportateur(s) de données: *[Identité et coordonnées du ou des exportateurs de données et, le cas échéant, de leur délégué à la protection des données et/ou de leur représentant dans l'Union européenne]* telles qu'indiquées dans le Contrat

Importateur(s) de données: *[Identité et coordonnées du ou des importateurs de données, y compris de toute personne de contact chargée de la protection des données]*

Telles qu'indiquées dans le Contrat.

B. DESCRIPTION DU TRANSFERT

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

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

Telles qu'indiquées dans les sections 1 et 3 de l'Information sur le Traitement de Données

Catégories de données à caractère personnel transférées

Telles qu'indiquées dans les sections 1 et 3 de l'Information sur le Traitement de Données

Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, telles que la limitation stricte des finalités, les restrictions d'accès (notamment l'accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données, les restrictions applicables aux transferts ultérieurs ou les mesures de sécurité supplémentaires.

Telles qu'indiquées dans les sections 1 et 3 de l'Information sur le Traitement de Données

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

Telle qu'indiquée dans les sections 1 et 3 de l'Information sur le Traitement de Données

Nature du traitement

Telle qu'indiquée dans les sections 1 et 3 de l'Information sur le Traitement de Données

Finalité(s) du transfert et du traitement ultérieur des données

Telle(s) qu'indiquée(s) dans les sections 1 et 3 de l'Information sur le Traitement de Données

Durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, critères utilisés pour déterminer cette durée

Telle qu'indiquée dans les sections 1 et 3 de l'Information sur le Traitement de Données

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

Tels qu'indiqués dans les sections 1 et 3 de l'Information sur le Traitement de Données

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

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

Indiquez la ou les autorités de contrôle compétentes conformément à la clause 13

L'Autorité de contrôle compétente pour les Pays-Bas, la Autoriteit Persoonsgegevens (AP) (sauf disposition contraire en application de la clause 13)

ANNEXE II

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

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

NOTE EXPLICATIVE:

Les mesures techniques et organisationnelles doivent être décrites en termes spécifiques (et non généraux). Voir également le commentaire général à la première page de l'appendice, en particulier en ce qui concerne la nécessité d'indiquer clairement les mesures qui s'appliquent à chaque transfert/ensemble de transferts.

Description des mesures techniques et organisationnelles mises en œuvre par le ou les importateurs de données (y compris toute certification pertinente) pour garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

Telles que décrites à la section 2 de l'Information sur le Traitement de Données

ANNEXE III

LISTE DES SOUS-TRAITANTS ULTÉRIEURS

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

NOTE EXPLICATIVE:

La présente annexe doit être remplie pour les modules 2 et 3, en cas d'autorisation spécifique de sous-traitants ultérieurs [clause 9, paragraphe a), option 1]

Non applicable
