CONTRAT DE TRAITEMENT DES DONNÉES POUR LES SERVICES SAP CLOUD

1. PRÉAMBULE

1.1 Annexe.

Le présent document, avec la Pièce jointe 1 et les Appendices 1 et 2 (l'« **Annexe** »), fait partie intégrante du Contrat par le biais de sa référence dans le Formulaire de commande signé par le Client. La présente Annexe fait office de contrat écrit de traitement des données entre SAP et, sous réserve de la Section 1.2 ci-dessous, le Responsable du traitement qui fournit des Données à caractère personnel en rapport avec son utilisation du Service Cloud. Il définit en outre les mesures techniques et organisationnelles applicables que SAP met en œuvre et gère en vue de protéger les Données à caractère personnel conservées dans le système de production du Service Cloud.

1.2 Relation contractuelle directe.

(a) Si le traitement des Données personnelles par SAP est effectué dans l'EEE, la présente Annexe s'applique entre SAP et le Client. Dans un tel cas, le Client est chargé de transférer les conditions établies dans la présente Annexe à ses Sociétés affiliées.

(b) Si le Client et/ou ses Sociétés Affiliées sont situés dans l'EEE, ou que ses Sous-traitants traitent ou accèdent aux Données à caractère personnel en dehors de l'EEE, les Sections 5.1 et 5.2 de la présente Annexe s'appliquent.

1.3 Formulaire de commande.

La conclusion du Contrat auquel la présente Annexe est intégrée sera effective à compter de la réception par SAP de l'un des documents suivants:

(a) Formulaire de commande original signé,

(b) Formulaire de commande signé au format PDF ou dans un format similaire; ou

(c) Formulaire de commande accepté par le biais de DocuSign ou de tout moyen similaire utilisé par SAP pour recevoir un Formulaire de commande émanant du Client.

Si le Client requiert une copie sous forme écrite de l'original de la présente Annexe ou, séparément, une copie électronique signée de ladite Annexe, il devra en faire la demande auprès de son commercial SAP.

1.4 Gouvernance.

Le Client agit en qualité de Responsable du traitement à l'égard des Données à caractère personnel de ses propres Utilisateurs autorisés ainsi que pour le compte et au nom de ses Sociétés affiliées ou tiers en leur qualité de Responsables du traitement autorisés par le Client à utiliser le Service. Le Client fait fonction d'interlocuteur unique pour SAP et assume la responsabilité exclusive quant à la coordination interne, l'examen et la transmission à SAP d'instructions ou demandes d'autres Responsables du traitement. SAP est exonéré de son obligation d'informer ou notifier un Responsable du traitement dès lors qu'il a fourni l'information ou la notification en question au Client. SAP est habilité à rejeter toutes demandes ou instructions fournies directement par un Responsable du traitement autre que le Client. Le Client garantit qu'il est autorisé à divulguer les Données à caractère personnel à SAP dans le cadre du Service Cloud conformément au Contrat. Le Client convient de protéger SAP contre des actions en justice intentées à son encontre ou à l'encontre de ses Sous-traitants qui découleraient d'une violation des obligations de protection des données du Client.

1.5 Indépendance des clauses.

Si une clause de la présente Annexe est déclarée inopérante ou inexécutoire par un tribunal d'une juridiction compétente, le caractère inopérant de ladite clause n'affectera pas les autres clauses de la présente Annexe, lesquelles conserveront leur plein effet.

2. FINALITÉS DU TRAITEMENT DES DONNÉES

2.1 Appendice 1.

Le Client et les Responsables du traitement des données respectifs sont tenus d'établir la finalité de la collecte, du traitement et de l'utilisation des données à caractère personnel conservées dans le cadre du Service Cloud. Sauf disposition contraire dans le Contrat, l'Appendice 1 de l'Annexe s'applique au traitement de données susmentionné.

2.2 Objet.

Les finalités du traitement de Données à caractère personnel par SAP et ses Sous-traitants en vertu de la présente Annexe se limitent à ce qui suit:

(a) Installation, exploitation, suivi et mise à disposition du Service Cloud, y compris l'infrastructure sous-jacente (matériel, logiciels, centres de données sécurisés, connectivité), en tant que Sous-traitant initial ou Sous-traitant ultérieur, tel que précisé dans le Contrat.

(b) Prestation de services de support technique en tant qu'obligation majeure de SAP en vertu du Contrat.

(c) Prestation de services de conseil en tant que prestation majeure de SAP, si et dans la mesure où lesdits services ont été convenus par les parties.

(d) Communication aux Utilisateurs autorisés tels que définis dans les conditions associées à un Service Cloud particulier.

(e) Exécution d'instructions du Client conformément aux Sections 3.1 et 3.2 ci-dessous.

3. OBLIGATIONS DE SAP

3.1 Instructions.

SAP s'engage à traiter les Données à caractère personnel exclusivement selon les instructions de chaque Responsable du traitement telles que communiquées par le Client. SAP est tenu de déployer des efforts commercialement raisonnables pour suivre et respecter les instructions transmises par le Client, dans la mesure où elles sont légalement imposées et techniquement faisables et ne requièrent pas d'apporter des modifications importantes aux fonctionnalités du Service Cloud ou aux progiciels sous-jacents. SAP s'engage à informer le Client si SAP considère qu'une instruction transmise par le Client constitue une violation de la Loi relative à la protection des données applicable. SAP n'est pas tenu de procéder à un examen juridique complet. S'il s'avère que SAP est dans l'incapacité de respecter une instruction, il doit en informer le Client dans les meilleurs délais (une communication par courrier électronique est autorisée).

3.2 Instructions basées sur les recours de la Personne concernée.

SAP peut, sur instruction du Client et avec la collaboration nécessaire de ce dernier, rectifier, effacer et/ou bloquer des Données à caractère personnel dès lors que les fonctionnalités du Service Cloud ne permettent pas au Client, à ses Responsables du traitement ou Utilisateurs autorisés de le faire eux-mêmes. Si SAP a besoin d'accéder à distance à l'un des systèmes du Client ou à une instance Client du Service Cloud pour exécuter une instruction ou apporter une assistance technique, par exemple par le partage d'application, le Client autorise par la présente SAP à procéder audit accès à distance. En outre, le Client doit désigner un interlocuteur qui, si nécessaire, accordera à SAP les droits d'accès requis.

3.3 Secret des données.

Pour le traitement de Données à caractère personnel, SAP et ses Sous-traitants ne doivent recourir qu'à des collaborateurs qui sont liés par l'obligation de respecter le secret des données ou le secret des télécommunications, dans la mesure applicable, conformément à la Loi relative à la protection des données. SAP doit former régulièrement en matière de sécurité et confidentialité des données les collaborateurs auxquels elle confère l'autorisation d'accéder à des Données à caractère personnel, et doit exiger de ses Sous-traitants qu'ils fassent de même.

3.4 Mesures techniques et organisationnelles.

(a) SAP doit, au minimum, mettre en place et maintenir les mesures techniques et organisationnelles appropriées décrites dans l'Appendice 2 de l'Annexe.

(b) L'Appendice 2 s'applique au système de production du Service Cloud pour préserver la sécurité des Données à caractère personnel et les protéger contre tout traitement non autorisé ou illégal et toute perte, destruction ou tout préjudice accidentel. Les environnements non productifs (par exemple, une instance de test du Service Cloud) procurent un niveau de sécurité inférieur et SAP recommande au Client de ne pas conserver de Données à caractère personnel dans de tels environnements non productifs.

(c) Étant donné que SAP fournit le Service Cloud à tous les clients de façon uniforme par l'intermédiaire d'une application hébergée basée sur Internet, toutes les mesures techniques et organisationnelles appropriées et en vigueur s'appliquent à la totalité de la clientèle de SAP hébergée à partir du même centre de données et abonnée au même Service Cloud. Le Client comprend et accepte que les mesures techniques et organisationnelles soient soumises à une évolution technique et à des développements et que des améliorations pour la protection des Données à caractère personnel seront automatiquement appliquées.

3.5 Vérification.

SAP doit régulièrement mettre à l'essai les mesures décrites dans l'Appendice 2. Si un Responsable du traitement estime que des mesures supplémentaires sont requises en vertu de la Loi relative à la protection des données applicable, le Client transmettra une instruction conformément à la Section 3.1 ci-dessus.

3.6 Notification d'une violation de la sécurité.

SAP doit informer le Client dans les meilleurs délais dès qu'il prend connaissance de perturbations graves affectant les opérations de traitement, ou de Violations de la sécurité qui sont liées au traitement de Données à caractère personnel et qui sont susceptibles, dans chaque cas, de porter un préjudice significatif aux intérêts des Personnes concernées.

3.7 Coopération.

Aux frais et à la demande du Client, SAP doit apporter une assistance raisonnable au Client ou autres Responsables du traitement pour répondre aux requêtes émanant de Personnes concernées individuelles et/ou d'une autorité de tutelle à l'égard du traitement de Données à caractère personnel en vertu des présentes.

3.8 Suppression.

À la fin du Contrat, SAP supprimera les Données à caractère personnel restant sur les serveurs qui hébergent le Service Cloud, à moins que la loi applicable ou le Contrat exige de les conserver. Les données conservées sont soumises aux clauses de confidentialité du Contrat.

4. SOUS-TRAITANTS

4.1 Utilisation autorisée.

(a) Le Client (agissant également pour le compte de ses Responsables du traitement) autorise SAP par les présentes (également aux fins de la Clause 11, paragraphe 1, des Clauses contractuelles types) à engager des sous-traitants pour le traitement de Données à caractère personnel (chacun, un « **Sous-traitant** ») (i) dans la mesure nécessaire pour exécuter les obligations contractuelles mises à sa charge par le Contrat et (ii) à condition que SAP demeure responsable de tous actes ou omissions de ses Sous-traitants dans la même mesure qu'il est responsable de ses propres actes et omissions en vertu des présentes.

(b) SAP transfère à ses Sous-traitants les obligations qui incombent à SAP en sa qualité de Sous-traitant initial (ou Sous-traitant ultérieur) vis-à-vis du Client et des Responsables du traitement concernés, telles que lesdites obligations sont exposées dans la présente Annexe.

(c) SAP s'engage à appliquer un processus de sélection visant à évaluer les pratiques de sécurité, de protection et de confidentialité d'un Sous-traitant vis-à-vis de la gestion des données, dans le cadre d'un programme de contrôle. Le Sous-traitant peut aussi être titulaire d'une certification de sécurité attestant que des mesures de sécurité adaptées sont en place s'agissant des services à fournir à SAP par le Sous-traitant.

(d) SAP communiquera par courrier électronique au Client, sur demande de ce dernier, le nom, l'adresse et le rôle de chaque Sous-traitant auquel il a recours pour fournir le Service Cloud.

4.2 Nouveaux Sous-traitants.

(a) SAP peut révoquer, remplacer ou désigner des Sous-traitants adaptés et fiables à son entière discrétion, conformément à la présente Section 4.2.

(b) SAP informera le Client par courrier électronique, à l'avance (sauf dans le cas des Remplacements d'urgence visés à la Section 4.3) de toutes les modifications affectant la liste des Sous-traitants. Si le Client ne manifeste pas son opposition conformément à la Section 4.2 (c) dans les trente jours qui suivent la réception de l'avis de SAP, le(s) nouveau(x) Sous-traitant(s) sera/seront réputé(s) accepté(s).

(c) Si le Client a un motif valable de s'opposer au recours par SAP à un Sous-traitant (par exemple si ce dernier n'est pas une Entité EEE et si le Client est contraint d'accomplir des démarches supplémentaires en qualité de Responsable du traitement avant le recours à un tel Sous-traitant), le Client est tenu d'en informer SAP par écrit dans les trente jours qui suivent la réception de l'avis de SAP. Si le Client s'oppose au recours à un tel Sous-traitant, SAP est en droit de résoudre ladite objection avec l'une des options suivantes (choisie par SAP à son entière discrétion): (i) SAP renonce à son idée de recourir au Sous-traitant à l'égard des Données à caractère personnel; ou (ii) SAP prend les mesures correctives demandées par le Client dans son objection (de manière à ce que l'objection du Client n'ait plus lieu d'être) et peut ensuite recourir au Sous-traitant à l'égard des Données à caractère personnel; ou (iii) SAP peut cesser de fournir ou le Client peut accepter de ne plus utiliser (à titre temporaire ou permanent) l'aspect particulier du Service Cloud qui impliquerait le recours au Sous-traitant à l'égard des Données à caractère personnel. Si aucune des options qui précèdent ne peut raisonnablement être choisie et si l'objection n'a pas été résolue dans les trente jours qui suivent la réception par SAP de l'objection du Client, chacune des parties est autorisée à résilier le Service Cloud affecté moyennant un préavis écrit raisonnable.

4.3 « Remplacement d'urgence » désigne le remplacement soudain d'un Sous-traitant lorsqu'un tel changement échappe au contrôle raisonnable de SAP (par exemple si le Sous-traitant cesse ses activités, met brusquement fin aux services qu'il fournissait à SAP ou viole ses obligations contractuelles envers SAP). Dans un tel cas, SAP informera le Client du Sous-traitant de remplacement dès que possible et déclenchera le processus menant à la désignation officielle dudit Sous-traitant en application de la Section 4.2 (b).

5. TRANSFERTS INTERNATIONAUX ET DISPOSITIONS SPÉCIFIQUES AUX PAYS

5.1 Transfert international.

Les Données à caractère personnel que SAP a reçues d'un Responsable du traitement situé dans l'EEE ne doivent pas être exportées par SAP ou ses Sous-traitants depuis un Centre de données (qu'il soit situé à l'intérieur ou à l'extérieur de l'EEE) vers un pays ou territoire extérieur à l'EEE, et ne peuvent pas faire l'objet d'un accès depuis un tel pays ou territoire (« **Transfert international** ») à moins que

(a) le destinataire ou le pays ou territoire depuis lequel il opère (où/depuis lequel il traite/accède aux Données à caractère personnel) est jugé assurer un niveau de protection adéquat des droits et libertés des personnes concernées en rapport avec le traitement des

Données à caractère personnel, selon la déclaration y afférente de la Commission Européenne, et sous réserve des restrictions de périmètre énoncées dans ladite déclaration; ou bien si

(b) le Transfert international vers une Entité non EEE est réalisé conformément à la Section 5.2 ci-dessous.

5.2 Clauses contractuelles types. Cadre multi-niveaux.

(a) Les Clauses contractuelles types jointes à la présente Annexe (« **Pièce jointe 1** ») et la Section 4 ci-dessus s'appliquent si le Contrat est conclu entre (i) un Client situé dans l'EEE ou (ii) un Client avec des Sociétés affiliées situées dans l'UE et une entité SAP située hors EEE.

(b) Pour tous les autres Transferts internationaux pour lesquels SAP utilise d'autres Entités non EEE (désignées en vertu de la Section 4 ci-dessus), SAP (représenté par SAP SE) a conclu avec chaque Entité non EEE les Clauses contractuelles types (version non modifiée) avant de traiter les Données à caractère personnel par le biais d'un Transfert international.

(c) Par les présentes, le Client adhère, et chaque Responsable du traitement peut adhérer, aux Clauses contractuelles types définies dans le paragraphe (b).

(d) Si le contrat direct précédent n'est pas disponible pour un Responsable du traitement en vertu d'une Loi relative à la protection des données obligatoire déterminée par SAP et le Client, le Responsable du traitement peut signer les Clauses contractuelles types fournies par SAP avec l'Entité non EEE pertinente (représentée par SAP SE).

(e) Si un tel droit direct pour appliquer les Clauses contractuelles directes à l'encontre de l'Entité non EEE n'existe pas pour le Responsable du traitement ou s'il est valablement contesté par un Sous-traitant, SAP est tenu de faire valoir les Clauses contractuelles types à l'encontre du Sous-traitant pour le compte du Responsable du traitement, conformément à la présente Annexe.

(f) Rien dans le présent Contrat ne saurait être interprété comme prévalant sur une Clause divergente des Clauses contractuelles types.

(g) Les Clauses contractuelles types sont régies par la loi de l'État membre dans lequel l'exportateur de données basé dans l'EEE est établi.

5.3 Dispositions spécifiques aux pays.

(a) **Australie.** (i) Aux fins de la présente Annexe - **« APP »** désigne les Principes de confidentialité Australiens (Australian Privacy Principles) de l'Annexe 1 à la loi « Privacy Amendment (Enhancing Privacy Protection) Act 2012 », qui a modifié la loi sur la confidentialité (« Privacy Act 1988 »); « **Responsable du traitement** » désigne une personne qui, seule, conjointement, ou associée à d'autres personnes, détermine les finalités et la manière de conduire le traitement actuel ou ultérieur des Données à caractère personnel; et « **Sous-traitant initial** » désigne toute personne (autre qu'un employé du Responsable du traitement) qui traite les Données à caractère personnel pour le compte du Responsable du traitement. (ii) Dans la mesure où un Responsable du traitement situé en Australie ou ses Utilisateurs autorisés souhaitent saisir des Données à caractère personnel dans le Service Cloud, le Client s'engage à obtenir au préalable le consentement de chaque Personne concernée avant d'effectuer un Transfert international, tel que visé dans la présente Annexe, si et dans la mesure où un tel consentement est requis en vertu de la loi australienne applicable en matière de protection des données. Le Client confirme par la présente avoir reçu les Données à caractère personnel et avoir informé les Personnes concernées au sujet de la divulgation desdites Données à caractère personnel conformément aux APP et à la loi sur la confidentialité (« Privacy Act 1988 »). Sur cette base, l'APP 8.1 est donc satisfait et ne devra donc pas s'appliquer en vertu de l'exception relative au « consentement éclairé » au titre de l'APP 8.2(b) (le « **Consentement éclairé** »). Dans la mesure où le Consentement éclairé ne s'applique pas, la présente Annexe fournit un cadre pour la protection des Données à caractère personnel des

Personnes concernées de nationalité australienne d'une façon qui est, globalement, substantiellement similaire à la protection des renseignements assurée par les APP et SAP accepte de consacrer auxdites Données à caractère personnel un niveau de protection similaire tel que défini dans les Sections 2, 3 et 6 de la présente Annexe (en vertu de l'exception relative à la « loi substantiellement similaire » dans le cadre de l'APP 8.2 (a)) (la « **Loi substantiellement similaire** »), ainsi, et sur cette base, l'APP 8.1 est satisfaite et ne s'applique donc pas en vertu de la Loi substantiellement similaire.

(b) **Autriche**. Dans la mesure où un Responsable du traitement situé en Autriche ou ses Utilisateurs autorisés souhaitent saisir dans le Service Cloud les données à caractère personnel d'entités légales (également considérées comme des données à caractère personnel dans la Loi fédérale autrichienne relative à la protection des données personnelles (DGS 2000)), le Client s'engage à obtenir au préalable le consentement (selon l'article 12, paragraphe 3 de la DGS 2000) desdites entités légales (Personne concernée) avant d'utiliser le Service Cloud, tel que décrit dans les présentes, pour une telle Personne concernée. SAP s'engage à accorder à de telles données à caractère personnel un niveau de protection similaire à celui exposé aux Sections 2, 0 et 6 de la présente Annexe.

(c) **Fédération de Russie**. Le Client ou les Sociétés affiliées du Client, en leur qualité de Responsables du traitement, demeurent les opérateurs des Données à caractère personnel des ressortissants Russes transmises à SAP en vue de leur traitement, et il leur incombe d'établir (i) si le Client sera en mesure de respecter la loi russe applicable en matière de protection des données dans le cadre de l'utilisation du Service Cloud qui implique le traitement de Données à caractère personnel de ressortissants russes et (ii) si le Service Cloud peut être utilisé au sein ou hors de la Fédération de Russie.

(d) **Singapour.** Conformément à la réglementation 10(2)(b) des réglementations relatives à la protection des Données à caractère personnel de 2014 (« Personal Data Protection Regulations 2014 »), sauf indication contraire dans le Formulaire de commande, les pays auxquels SAP est susceptible de transférer des Données à caractère personnel faisant partie des Données client dans le cadre de la mise à disposition du Service Cloud au titre du Contrat (à la date d'entrée en vigueur du Formulaire de commande signé par le Client) sont l'Australie, l'Autriche, le Brésil, la Bulgarie, le Canada, le Chili, la Chine, Hong Kong, la République tchèque, la France, l'Allemagne, la Hongrie, l'Inde, l'Irlande, Israël, la Malaisie, le Mexique, les Pays-Bas, le Pérou, les Philippines, la Pologne, la Fédération de Russie, Singapour, la Slovaquie, l'Afrique du Sud, la Corée du Sud, l'Espagne, la Suède, le Royaume-Uni et les États-Unis d'Amérique. SAP pourra ajouter de nouveaux pays à la liste de pays indiquée ci-dessus et en avisera le Client via la procédure applicable en cas de modification de la liste des Sous-traitants définie dans la Section (d) ci-dessus, ledit avis devra inclure le pays dans lequel se situe tout nouveau Sous-traitant. Ladite Section n'inclut pas nécessairement tous les pays auxquels SAP est susceptible de transférer des Données client selon les instructions du Client, ou bien les pays à partir desquels le Client, ses Utilisateurs autorisés ou ses Partenaires d'affaires accèdent au Service Cloud.

(e) **Corée du Sud.** Dans la mesure où un Responsable du traitement situé en République de Corée ou ses Utilisateurs autorisés souhaitent saisir dans le Service Cloud des Données à caractère personnel, le Client s'engage à obtenir au préalable le consentement de chaque Personne concernée avant d'effectuer un Transfert international, tel que stipulé dans la présente Annexe, si et dans la mesure où un tel consentement est requis en vertu de la Loi en matière de protection des données applicable en République de Corée. Le Client confirme par la présente avoir reçu les Données à caractère personnel et avoir informé les personnes concernées au sujet du transfert/traitement desdites données conformément à la loi applicable.

(f) **Suisse.** Dans la mesure où un Responsable du traitement situé en Suisse ou ses Utilisateurs autorisés souhaitent saisir dans le Service Cloud les données à caractère

personnel d'entités légales (également considérées comme des données à caractère personnel dans la Loi fédérale suisse relative à la protection des données), le Client s'engage à obtenir au préalable le consentement (selon l'article 6, paragraphe 2, alinéa b, de ladite Loi) desdites entités légales (**« Personne concernée »**) avant d'utiliser le Service Cloud, tel que décrit dans les présentes, pour une telle Personne concernée. SAP s'engage à accorder à de telles données à caractère personnel un niveau de protection similaire à celui exposé aux Sections 2, 0 et 6 de la présente Annexe.

(g) **Turquie.** Dans la mesure où un Responsable du traitement situé en Turquie ou ses Utilisateurs autorisés souhaitent saisir des Données à caractère personnel dans le Service Cloud, le Client s'engage à obtenir au préalable le consentement de chaque Personne concernée avant d'effectuer un Transfert international, tel que visé dans la présente Annexe, si et dans la mesure où un tel consentement est requis en vertu de la loi turque applicable en matière de protection des données. Le Client confirme par la présente avoir reçu les Données à caractère personnel et avoir informé les personnes concernées au sujet du transfert/traitement desdites données conformément à la loi applicable.

(h) **États-Unis**. À moins que SAP et le Client n'aient signé un accord entre partenaires d'affaires pour l'échange de renseignements de santé protégées (« protected health information » ou « **PHI** ») telles que définies dans la loi américaine « Health Insurance Portability and Accountability Act » de 1996 et ses modifications ultérieures, en rapport avec le Service Cloud, le Client déclare par la présente qu'il ne transmettra pas de PHI vers le Service Cloud et qu'il ne sollicitera pas de tels renseignements auprès de partenaires ou de clients dans le cadre de l'utilisation du Service Cloud.

6. CERTIFICATIONS ET VÉRIFICATIONS

6.1 Certifications et rapports de vérification.

Pour les systèmes de production qui exécutent le Service Cloud et pendant la durée du Contrat, SAP est tenu de gérer, à ses frais, les certifications ou rapports de vérification applicables.

(a) Au minimum, SAP a recours aux services d'un vérificateur tiers indépendant reconnu à l'échelle internationale pour l'examen des mesures mises en place en vue d'assurer la protection du Service Cloud: (i) les certifications peuvent se fonder sur la norme ISO 27001 ou sur d'autres normes (périmètre défini dans le certificat); (ii) pour certains Services SAP Cloud, SAP fournit également un rapport valide ISAE3402 ou SSAE16-SOC 1 type 2 et/ou ISAE3000 ou SSAE16-SOC 2 type 2. Sur demande du Client, SAP informera le Client concernant les certifications applicables et normes de vérification disponibles pour le Service Cloud concerné.

(b) Sur demande du Client, le vérificateur tiers ou SAP, selon le cas, devra fournir les rapports de vérification SOC (relatifs aux contrôles des sociétés de services) et les certifications ISO.

6.2 Vérifications client.

Conformément à la Section 6.4 ci-dessous et en vertu de la Loi obligatoire relative à la protection des données, le Client (ou un vérificateur tiers indépendant agissant pour son compte, faisant l'objet d'obligations de confidentialité similaires à celles prévues dans le Contrat), peut vérifier l'environnement de contrôle et les pratiques de sécurité de SAP pertinentes relativement aux Données à caractère personnel traitées en vertu des présentes pour le Client si:

(a) SAP n'a pas présenté de justificatifs suffisants attestant de sa conformité en vertu de la Section 6.1;

(b) un événement visé à la Section 3.6 ci-dessus est survenu;

(c) le Client ou un autre Responsable du traitement a des motifs raisonnables de suspecter que SAP manque à ses obligations en vertu de la présente Annexe;

(d) une vérification ultérieure est requise par le régulateur ou l'autorité de protection des données ayant compétence sur le Client ou sur un autre Responsable du traitement (par

exemple dans le cas où un organisme chargé de l'application des lois est autorisé à effectuer une vérification d'un Responsable du traitement si les Données à caractère personnel ont été traitées sur le site du Responsable du traitement).

6.3 Coopération.

SAP s'engage à apporter une aide raisonnable au Client lors de ses processus de vérification en vertu de la Loi relative à la protection des données et à lui fournir les renseignements nécessaires.

6.4 Restrictions relatives à la vérification.

(a) Sauf indication contraire dans la Loi obligatoire relative à la protection des données, une vérification sera réalisée au maximum une fois tous les douze mois dans le cadre de la Section (b).

(b) Une vérification ne devra pas durer plus de trois jours d'ouverture.

(c) Le Client est tenu d'informer SAP moyennant un préavis écrit raisonnable (d'au moins 60 jours à moins qu'une autorité de protection des données n'exige du Client un contrôle antérieur en vertu d'une Loi obligatoire relative à la protection des données).

(d) Le Client et SAP doivent convenir mutuellement à l'avance du périmètre et du programme de la vérification. La vérification doit, dans la mesure du possible, s'appuyer sur des certifications et sur des rapports de vérification ou sur toutes autres vérifications disponibles afin de confirmer que SAP est conforme à la présente Annexe et d'éviter toute vérification répétitive.

(e) Le Client est tenu de conduire la vérification en temps, lieu et manière raisonnables et de fournir à SAP une copie du rapport de vérification.

(f) Chacune des parties doit assumer ses propres frais relatifs à la vérification en vertu de la Section (b), en revanche, le Client doit également prendre à sa charge les frais de SAP pour les collaborateurs internes de SAP requis pour conduire une vérification en vertu de la Section 6.2 (d) ou en vertu de la Loi obligatoire relative à la protection des données. Les frais d'un collaborateur interne de SAP doivent se fonder sur la base des tarifs de services professionnels quotidiens alors en vigueur et applicables au Client, ou, en l'absence d'un tel accord, sur la base de la liste de prix de SAP.

(g) S'il est établi suite à une vérification, que SAP a manqué à ses obligations en vertu de la présente Annexe (la « **Conclusion** »), SAP devra immédiatement y remédier. SAP doit déterminer à son entière discrétion quelles mesures sont les plus appropriées de manière à assurer sa conformité au titre de la présente Annexe.

7. DÉFINITIONS

Les termes débutant par une majuscule utilisés dans les présentes, tels que Société affiliée, Contrat, Client, Utilisateur autorisé (parfois également désigné comme un Utilisateur ou Utilisateur nommé), Formulaire de commande ou Service Cloud (parfois également désigné comme Service), ont la signification qui leur est donnée dans le Contrat.

7.1 **« Centre de données »** désigne le lieu où l'instance de production du Service Cloud est hébergée pour le Client dans sa région, tel que publié sur la page**:** http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html ou notifié au Client ou convenu par ailleurs dans un Formulaire de commande.

7.2 Le terme « **Responsable du traitement** » a la signification qui lui est donnée dans la Loi relative à la protection des données applicable.

7.3 Le terme « **Exportateur de données** », tel qu'utilisé dans les Clauses contractuelles types, désigne le Client indiqué dans un Formulaire de commande ou son/ses Responsable(s) du traitement.

7.4 Le terme « **Importateur de données** », tel qu'utilisé dans les Clauses contractuelles types, désigne toute Entité non EEE applicable.

7.5 Le terme « **Sous-traitant initial** » a la signification qui lui est donnée dans la Loi relative à la protection des données applicable.

7.6 Le terme « **Loi relative à la protection des données applicable** » désigne la législation protégeant les droits et libertés fondamentaux des personnes et, en particulier, leur droit à la vie privée concernant le traitement des Données à caractère personnel en vertu du Contrat. SAP doit respecter les obligations supplémentaires définies dans un Formulaire de commande requises en vertu de lois de protection des données locales d'application obligatoire qui s'appliquent à SAP en sa qualité de Sous-traitant initial.

7.7 Le terme « **Personne concernée** »désigne une personne physique ou une entité légale identifiée ou identifiable (selon la définition qui en est donnée dans la Loi relative à la protection des données applicable).

7.8 Le terme « **EEE** » désigne l'Espace économique européen ainsi que tout pays pour lequel la Commission Européenne a publié une décision à caractère suffisant tel que publié sur http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

7.9 Le terme « **Sous-traitant européen** » désigne un Sous-traitant qui traite physiquement des Données à caractère personnel dans l'UE, en Islande, au Liechtenstein, en Norvège ou en Suisse.

7.10 Le terme « **Entité non EEE** » désigne toute entité ou Sous-traitant de SAP constitué(e) en personne morale en dehors de l'EEE, soit dans un pays qui n'assure pas un niveau de protection adéquat tel que déterminé par la Commission européenne.

7.11 Le terme « **Données à caractère personnel** » a la signification qui lui est donnée dans la Loi relative à la protection des données et, aux fins de la présente Annexe, comprend uniquement les données à caractère personnel saisies par le Client ou ses Utilisateurs autorisés dans le Service Cloud ou obtenues via leur utilisation du Service ou fournies à ou obtenues par SAP ou ses Sous-traitants en vue de fournir des services de support conformément au Contrat. Les Données à caractère personnel constituent un sous-ensemble de Données client et leur définition vaut dès lors qu'une Loi relative à la protection des données s'applique.

7.12 Le terme « **SAP** » désigne l'entité SAP qui est partie au Formulaire de commande auquel la présente Annexe est intégrée.

7.13 Le terme « **Violation de la sécurité** » désigne tout acte ou omission de SAP ou de ses Sous-traitants qui conduit à une divulgation non autorisée de Données à caractère personnel, enfreignant les mesures décrites dans l'Appendice 2, ou un incident similaire relativement auquel le Responsable du traitement est légalement tenu d'informer la Personne concernée ou l'autorité de protection des données compétente.

7.14 Le terme « **Clauses contractuelles types** », parfois également appelé « Clauses du modèle UE », désigne les (Clauses contractuelles types (sous-traitants)) basées sur la Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers, en vertu de la Directive 95/46/CE (notifiées dans le document C (2010) 593), ou toute version ultérieure qui en est publiée par la Commission (laquelle s'appliquera automatiquement), en ce compris les Appendices 1 et 2 jointes aux présentes.

7.15 Le terme « **Sous-traitant** », tel qu'utilisé dans les Clauses contractuelles types et dans la présente Annexe, désigne les Sociétés affiliées de SAP et les sous-traitants tiers engagés par SAP ou par des Sociétés affiliées de SAP conformément à la Section 4.

8. ACCÈS UE (OPTION)

8.1 Service Cloud éligible.

Par dérogation à la Section 5.1 de la présente Annexe, SAP accepte de fournir un Accès UE au Service Cloud si et dans la mesure où cela a été convenu dans le Formulaire de commande. Le Client comprend que l'Accès UE est fourni uniquement pour les services éligibles à l'Accès UE, tels que déterminés périodiquement par SAP, qui sont hébergés par SAP dans l'UE.

8.2 Site du centre de données.

À la Date d'entrée en vigueur du Formulaire de commande et par dérogation à toute clause conflictuelle du Formulaire de commande, les Centres de données utilisés pour héberger des Données à caractère personnel dans le Service Cloud commandé sont situés sur le territoire de l'EEE ou en Suisse. SAP s'engage à ne pas migrer l'instance Client vers un Centre de données en dehors du territoire de l'EEE ou de la Suisse sans l'accord écrit préalable du Client (courriel autorisé). Si SAP prévoit de migrer l'instance Client vers un centre de données au sein de l'EEE ou en Suisse, SAP doit en informer le Client par écrit (courriel autorisé) au plus tard trente jours avant la migration planifiée.

8.3 Accès UE.

À la demande du Client, SAP a accepté de s'abstenir de recourir à des Sous-traitants autres que des Sous-traitants européens pour fournir le support des systèmes de production du Service Cloud dans la mesure où un tel support peut requérir l'accès à des Données à caractère personnel, que ledit accès ait lieu ou non.

8.4 Exclusion.

Les Données personnelles suivantes ne sont pas soumises à l'accès UE:

(a) Coordonnées de l'auteur d'un message ou avis de demande d'assistance et/ou d'incident, lors du dépôt d'un message de demande d'assistance et/ou d'incident.

(b) Toutes autres Données personnelles envoyées par le Client lors du dépôt d'un message de demande d'assistance et/ou d'incident. Le Client peut choisir de ne pas transmettre de telles Données personnelles lors du dépôt d'un message de demande d'assistance et/ou d'incident. Si de telles données sont nécessaires pour le processus de gestion des incidents, le Client devra rendre anonymes lesdites Données personnelles préalablement à toute transmission du message d'incident à SAP.

(c) Données personnelles dans des systèmes non productifs.

Les Données personnelles qui ne sont pas soumises à l'Accès UE seront uniquement transférées ou rendues accessibles à SAP ou à ses Sous-traitants conformément à la Section 5.

Annexe 1
CLAUSES CONTRACTUELLES TYPES (SOUS-TRAITANTS)[1]

Au sens de l'Article 26(2) de la Directive 95/46/EC concernant le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers ne pouvant pas garantir un niveau adéquat de protection des données,

Le Client et/ou les Sociétés affiliées du Client basés dans l'UE selon la signification exposée à la Section 1.2 (b) du CONTRAT DE TRAITEMENT DES DONNÉES (dans les Clauses ci-après, désignés par le terme « **Exportateur de données** »)

et

SAP SE en tant que représentation des Entités non EEE selon la signification exposée à la Section 5.2 (b) du CONTRAT DE TRAITEMENT DES DONNÉES (dans les Clauses ci-après, désignés par le terme « **Importateur de données** »)

désignés séparément en tant que « partie »; conjointement en tant que « parties »,

ONT CONCLU les Clauses contractuelles suivantes (les Clauses) afin de fournir une protection adéquate conformément à la protection de la confidentialité et des droits et libertés fondamentaux des personnes physiques pour le transfert des données à caractère personnel de l'exportateur de données vers l'importateur de données, comme indiqué dans l'Appendice 1.

Clause 1
Définitions

Au sens des présentes Clauses:

(a) Les termes « données à caractère personnel », « catégories spéciales de données », « processus/traitement », « responsable du traitement », « responsable », « personne concernée » et « autorité de contrôle » revêtent la même signification que dans la Directive 95/46/EC du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données et à la libre circulation desdites données;
(b) Le terme « exportateur de données » désigne le responsable du traitement transférant les données à caractère personnel;
(c) Le terme « importateur de données » désigne le responsable approuvant la réception des données à caractère personnel transférées par l'exportateur de données et destinées au traitement pour son compte après le transfert conformément à ses instructions et aux termes des Clauses. Il n'est pas soumis à un système de pays tiers, garantissant ainsi une protection adéquate au sens de l'Article 25(1) de la Directive 95/46/EC;
(d) Le terme « sous-traitant » désigne tout responsable embauché par l'importateur de données ou tout autre sous-traitant de l'importateur de données acceptant de recevoir de l'importateur de données ou de tout autre sous-traitant de l'importateur de données des données à caractère personnel destinées exclusivement à la réalisation des activités de traitement pour le compte de l'exportateur de données après le transfert conformément à ses instructions, aux termes des Clauses et aux termes des contrats de sous-traitance écrits;

[1] Conformes à la décision de la Commission européenne du 5 février 2010 (2010/87/EU)

(e) Le terme « loi applicable en matière de protection des données » désigne la législation protégeant les droits et libertés fondamentaux des personnes physiques et, en particulier, le droit à la confidentialité conformément au traitement des données à caractère personnel applicable à un responsable du traitement dans l'État membre dans lequel l'exportateur de données est établi;
(f) Le terme « mesures de sécurité techniques et organisationnelles » désigne les mesures visant à protéger les données à caractère personnel contre toute destruction accidentelle ou illégale ou perte accidentelle, altération, divulgation ou accès non autorisés, en particulier dans le cas où le traitement implique la transmission de données sur un réseau, ainsi que contre toute autre forme illégale de traitement.

Clause 2
Détails du transfert

Les détails du transfert et en particulier les catégories spéciales de données à caractère personnel, le cas échéant, sont indiqués dans l'Appendice 1 qui fait partie intégrante des Clauses.

Clause 3
Clause concernant le tiers bénéficiaire

1. La personne concernée peut faire appliquer la présente Clause, la Clause 4(b) à (i), la Clause 5(a) à (e) et (g) à (j), la Clause 6(1) à (2), la Clause 7, la Clause 8(2) et les Clauses 9 à 12 à l'encontre de l'exportateur de données en tant que tiers bénéficiaire.

2. La personne concernée peut faire appliquer la présente Clause, la Clause 5(a) à (e) et (g), la Clause 6, la Clause 7, la Clause 8(2) et les Clauses 9 à 12 à l'encontre de l'importateur de données, dans les cas où l'exportateur de données a matériellement disparu, a cessé d'exister en droit à moins que l'ensemble de ses obligations juridiques n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, à laquelle reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre laquelle la personne concernée peut donc faire appliquer lesdites Clauses.

3. La personne concernée peut faire appliquer la présente Clause, la Clause 5(a) à (e) et (g), la Clause 6, la Clause 7, la Clause 8(2) et les Clauses 9 à 12 à l'encontre du sous-traitant, dans les cas où l'exportateur et l'importateur de données ont tous les deux matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables à moins que l'ensemble des obligations juridiques de l'exportateur de données n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, à laquelle revient par conséquent les droits et les obligations de l'exportateur de données, et contre laquelle la personne concernée peut donc faire appliquer lesdites Clauses. Ladite responsabilité du sous-traitant en tant que tiers doit être limitée à ses propres activités de traitement conformément auxdites Clauses.

4. Les parties ne s'opposent pas à ce que la personne concernée soit représentée par une association ou un autre organisme si elle en exprime le souhait et si la législation nationale l'autorise.

Clause 4
Obligations de l'exportateur de données

L'exportateur de données consent et s'engage comme suit:

(a) le traitement, y compris le transfert lui-même, des données à caractère personnel a été et continuera à être réalisé conformément aux dispositions pertinentes de la loi applicable en

matière de protection des données (et, le cas échéant, a été notifié aux autorités de l'État membre dans lequel l'exportateur de données est établi) et n'enfreint pas les dispositions pertinentes dudit État;

(b) il a chargé, et chargera pendant toute la durée des services de traitement de données à caractère personnel, l'importateur de données de traiter les données à caractère personnel transférées pour le compte exclusif de l'exportateur de données et conformément à la loi applicable en matière de protection des données et aux Clauses;

(c) l'importateur de données offrira suffisamment de garanties en ce qui concerne les mesures de sécurité techniques et organisationnelles spécifiées dans l'Appendice 2 au présent contrat;

(d) après vérification des exigences de la loi applicable en matière de protection des données, il veillera à ce que les mesures de sécurité conviennent à la protection des données à caractère personnel contre toute destruction accidentelle ou illégale ou perte accidentelle, altération, divulgation ou accès non autorisés, en particulier dans le cas où le traitement implique la transmission de données sur un réseau, ainsi que contre toute autre forme illégale de traitement. Lesdites mesures garantissent un niveau de sécurité adéquat par rapport aux risques présentés par le traitement et la nature des données nécessitant une protection et en ce qui concerne la technologie et le coût de leur implémentation;

(e) il garantira la conformité aux mesures de sécurité;

(f) si le transfert implique les catégories spéciales de données, la personne concernée a été informée ou sera informée, avant ou dès que possible après le transfert, que ses données pourraient être transmises à un pays tiers ne présentant pas de protection adéquate au sens de la Directive 95/46/EC;

(g) il transmettra toute notification reçue de l'importateur de données ou tout sous-traitant dans le cadre de la Clause 5(b) et de la Clause 8(3) à l'autorité de contrôle de protection des données si l'exportateur de données décide de poursuivre le transfert ou de lever la suspension;

(h) il met à la disposition des personnes concernées une copie des présentes Clauses sur demande, à l'exception de l'Appendice 2, et une description succincte des mesures de sécurité, ainsi qu'une copie de tout contrat concernant les services de sous-traitance ayant été effectués conformément aux Clauses, à moins que les Clauses ou le contrat ne contiennent des informations commerciales, auquel cas de telles informations commerciales peuvent être supprimées;

(i) en cas de sous-traitance, l'activité de traitement est réalisée conformément à la Clause 11 par un sous-traitant fournissant au moins le même niveau de protection pour les données à caractère personnel et les droits de la personne concernée que celui fourni par l'importateur de données conformément auxdites Clauses;

(j) il garantit la conformité avec la Clause 4(a) à (i).

Clause 5

Obligations de l'importateur de données

L'importateur de données consent et s'engage comme suit:

(a) il traite les données à caractère personnel uniquement pour le compte de l'exportateur de données et conformément aux instructions et aux Clauses; s'il ne lui est pas possible d'assurer une telle conformité pour quelque raison que ce soit, il accepte d'informer dans les plus brefs délais l'exportateur de données de son incapacité de conformité, auquel cas l'exportateur de données est autorisé à suspendre le transfert de données et/ou à résilier le présent contrat;

(b) il n'a aucune raison de croire que la législation applicable l'empêche de répondre aux instructions reçues de l'exportateur de données et à ses obligations en vertu du contrat. En cas de modification apportée à la législation étant susceptible d'avoir des effets indésirables importants

sur les garanties et obligations fournies par lesdites Clauses, il avertira l'exportateur de données dans les plus brefs délais de la modification dès qu'il en aura pris connaissance, auquel cas l'exportateur de données est autorisé à suspendre le transfert de données et/ou à résilier le présent contrat;

(c) il a implémenté les mesures de sécurité techniques et organisationnelles mentionnées dans l'Appendice 2 avant de traiter les données à caractère personnel qui ont été transférées;

(d) il avertira dans les plus brefs délais l'exportateur de données de:

(i) toute requête juridiquement contraignante concernant la divulgation de données à caractère personnel par une autorité chargée de l'application des lois, à moins qu'il n'existe un autre type d'interdiction, comme une interdiction en vertu du droit pénal dans le but de préserver la confidentialité d'une enquête judiciaire;
(ii) tout accès accidentel ou non autorisé; et
(iii) toute requête reçue directement des personnes concernées sans répondre à ladite requête, à moins qu'une autre autorisation n'ait été prononcée;

(e) il traitera correctement et dans les plus brefs délais toutes les demandes de l'exportateur de données relatives au traitement des données à caractère personnel faisant l'objet du transfert et se rangera à l'avis de l'autorité de contrôle en ce qui concerne le traitement des données transférées;

(f) à la demande de l'exportateur de données, il soumettra ses installations de traitement de données à une vérification des activités de traitement couvertes par les présentes Clauses qui devra être réalisé par l'exportateur de données ou un organe de contrôle composé de membres indépendants possédant les qualifications professionnelles requises, soumis à une obligation de confidentialité et sélectionnés par l'exportateur de données, le cas échéant, en accord avec l'autorité de contrôle;

(g) il mettra à la disposition de la personne concernée une copie des présentes Clauses ou tout contrat de sous-traitance existant sur demande, à moins que les Clauses ou le contrat ne contiennent des informations commerciales, auquel cas de telles informations commerciales peuvent être supprimées, à l'exception de l'Appendice 2 qui doit être remplacé par une description succincte des mesures de sécurité dans les cas où la personne concernée se trouve dans l'incapacité d'obtenir une copie de l'exportateur de données;

(h) en cas de sous-traitance, il veillera au préalable à informer l'exportateur de données et à obtenir l'accord écrit de ce dernier;

(i) les services de traitement fournis par le sous-traitant seront conformes à la Clause 11;

(j) il enverra dans les plus brefs délais une copie de tout contrat de sous-traitance conclu avec l'exportateur de données en vertu des présentes Clauses.

Clause 6
Responsabilité

1. Les parties consentent que toute personne concernée ayant subi un préjudice résultant de la violation des obligations désignées dans la Clause 3 ou la Clause 11 par une des parties ou par un sous-traitant a le droit d'obtenir de l'exportateur de données réparation au préjudice subi.

2. Si une personne concernée n'est pas en mesure d'intenter l'action de réparation conformément au paragraphe 1 contre l'exportateur de données, pour manquement par l'importateur de données ou du sous-traitant à l'une ou l'autre de ses obligations mentionnées dans la Clause 3 ou la Clause 11, car l'exportateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable à moins que l'ensemble des obligations juridiques de l'exportateur de données n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, à laquelle revient par conséquent les droits et les obligations de l'exportateur de données, et contre laquelle la personne concernée peut donc faire appliquer lesdites Clauses.

L'importateur de données ne peut se prévaloir d'un manquement par le sous-traitant à ses obligations dans le but de ne pas assurer ses propres responsabilités.

3. Si une personne concernée n'est pas en mesure d'intenter une action conformément aux paragraphes 1 et 2 contre l'exportateur de données ou l'importateur de données, pour manquement par le sous-traitant à l'une ou l'autre de ses obligations mentionnées dans la Clause 3 ou la Clause 11, car l'exportateur et l'importateur de données ont tous les deux matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables à moins que l'ensemble des obligations juridiques de l'exportateur de données n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, à laquelle revient par conséquent les droits et les obligations de l'exportateur de données, et contre laquelle la personne concernée peut donc faire appliquer lesdites Clauses. La responsabilité du sous-traitant doit être limitée à ses propres activités de traitement conformément auxdites Clauses.

Clause 7
Médiation et juridiction

1. L'importateur de données consent que si la personne concernée invoque contre lui les droits de tiers bénéficiaire et/ou intente l'action de réparation pour les préjudices en vertu des Clauses, l'importateur de données acceptera la décision de la personne concernée:

(a) de soumettre le litige à une médiation représentée par une personne indépendante ou, le cas échéant, par une autorité de contrôle;
(b) de soumettre le litige aux tribunaux de l'État membre dans lequel l'exportateur de données est établi.

2. Les parties consentent que le choix fait de la personne concernée ne portera pas préjudice à ses droits matériels ou procéduraux pour chercher un recours conformément aux autres clauses de la loi nationale ou internationale.

Clause 8
Coopération avec les autorités de contrôle

1. L'exportateur de données consent à déposer une copie du présent contrat auprès de l'autorité de contrôle si nécessaire ou si un tel dépôt est requis en vertu de la loi applicable en matière de protection des données.

2. Les parties consentent que l'autorité de contrôle a le droit d'effectuer un audit de l'importateur de données et de chacun de ses sous-traitants, dans le même périmètre et sous les mêmes conditions appliquées à un audit de l'exportateur de données en vertu de la loi applicable en matière de protection des données.

3. L'importateur de données s'engage à informer dans les meilleurs délais l'exportateur de données concernant l'existence d'une législation applicable à son activité ou celle de tout sous-traitant entravant la réalisation d'un audit de l'importateur de données ou sous-traitant conformément au paragraphe 2. Dans un tel cas, l'exportateur de données est autorisé à prendre les mesures prévues dans la Clause 5(b).

Clause 9
Droit applicable

Les Clauses sont régies par la loi de l'État membre dans lequel l'exportateur de données est établi.

Clause 10
Modifications du contrat

Les parties s'engagent à ne pas modifier les présentes Clauses. La présente condition n'empêche pas les parties d'ajouter des clauses concernant des problèmes relevant de l'activité commerciale si nécessaire, dans la mesure où elles ne contredisent pas la Clause.

Clause 11
Sous-traitance

1. L'importateur de données ne doit sous-traiter aucune de ses opérations de traitement réalisées pour le compte de l'exportateur de données en vertu des présentes Clauses sans le consentement écrit et préalable de l'exportateur de données. Dans le cas où l'importateur de données sous-traite ses obligations en vertu des présentes Clauses avec le consentement de l'exportateur de données, il doit le faire uniquement en concluant un accord écrit avec le sous-traitant imposant les mêmes obligations au sous-traitant que celles qui lui sont imposées dans les présentes Clauses. Dans le cas où le sous-traitant manque à ses obligations de protection des données en vertu dudit contrat écrit, l'importateur de données s'engage à rester totalement responsable envers l'exportateur de données concernant l'exécution des obligations du sous-traitant en vertu dudit contrat.

2. Le contrat écrit et préalable entre l'importateur de données et le sous-traitant doit également prévoir une clause concernant un tiers bénéficiaire telle que définie dans la Clause 3 pour les cas où la personne concernée n'est pas en mesure d'intenter l'action de réparation mentionnée au paragraphe 1 de la Clause 6 contre l'exportateur de données ou l'importateur de données, car ils ont tous les deux matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables et aucune entité leur succédant n'assume l'ensemble des obligations juridiques de l'exportateur ou de l'importateur de données transférées par contrat ou par effet de la loi. Ladite responsabilité du sous-traitant en tant que tiers doit être limitée à ses propres activités de traitement conformément auxdites Clauses.

3. Les clauses relevant des aspects de la protection des données pour la sous-traitance du contrat mentionné au paragraphe 1 sont régies par la loi de l'État membre dans lequel l'exportateur de données est établi, à savoir l'Allemagne.

4. L'exportateur de données conservera une liste des contrats de sous-traitance conclus en vertu des présentes Clauses et notifiés par l'importateur de données conformément à la Clause 5(j) qui sera mise à jour au moins une fois par an. La liste sera mise à la disposition de l'autorité de contrôle de protection des données de l'exportateur de données.

Clause 12

Obligations après résiliation des services de traitement des données à caractère personnel

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

2. L'importateur de données et le sous-traitant garantissent qu'à la demande de l'exportateur de données et/ou de l'autorité de contrôle, ils soumettront leurs installations de traitement de données à un audit des mesures mentionné au paragraphe 1.

APPENDICE 1 AU CONTRAT DE TRAITEMENT DE DONNÉES ET AUX CLAUSES CONTRACTUELLES TYPES.

Les Parties peuvent fournir des précisions supplémentaires dans un Formulaire de commande ou Supplément, si nécessaire, ou les ajuster dans les descriptions fournies par le Client qui figurent ci-dessous.

Exportateur de données
L'Exportateur de données s'est abonné au Service SAP Cloud qui confèrent à ses Utilisateurs autorisés le droit de saisir, modifier, utiliser, supprimer ou traiter selon d'autres modalités des Données à caractère personnel, tel que prévu dans le Contrat.

Importateur de données
SAP et ses Sous-traitants fournissent le Service Cloud, ce qui inclut le support suivant:
Les Sociétés affiliées de SAP à l'échelle internationale apportent leur soutien aux centres de données du Service SAP Cloud à distance depuis des sites de SAP, par exemple à St. Leon-Rot (Allemagne), en Inde ou depuis d'autres sites où SAP emploie du personnel pour la fonction Opérations/Services Cloud. Le support inclut, mais de façon non limitative:

- le suivi du Service Cloud et de l'infrastructure sous-jacente;
- la sauvegarde et la restauration des Données client conservées dans le Service Cloud;
- le lancement et le développement de correctifs, de nouvelles mises à jour et mises à niveau du Service Cloud et de l'infrastructure sous-jacente;
- la correction des erreurs liées aux équipements réseau, de stockage et aux serveurs;
- le suivi de la base de données, la correction des erreurs, les activités de gestion quotidiennes des bases de données, y compris le redimensionnement des bases de données de production, la création d'index, le réglage des performances, la gestion des correctifs; la gestion des bases de données de secours et les projets liés aux fonctions des bases de données;
- la gestion de la sécurité, l'aide à la détection des intrusions réseau, la réalisation de tests de pénétration.

Les Sociétés affiliées de SAP fournissent également un support lorsqu'un Client soumet une demande de support car le Service Cloud n'est pas disponible ou ne fonctionne pas comme prévu pour plusieurs ou pour tous les Utilisateurs autorisés (incident): SAP fournit une réponse par téléphone, apporte des corrections basiques aux erreurs, transmet et gère les messages de support dans un système de suivi distinct de l'instance de production du Service Cloud.

Personnes concernées
Les Données à caractère personnel transférées s'appliquent aux catégories de personnes concernées suivantes:
Sauf décision contraire de l'Exportateur de données, les Personnes concernées peuvent comprendre des employés, contractuels, partenaires d'affaires ou autres individus dont des Données à caractère personnel sont conservées dans le cadre du Service Cloud.

Catégories de données
Les Données à caractère personnel transférées concernent les catégories suivantes de données:
Le Client détermine les catégories de données par Service Cloud souscrit. Les champs de données du Client peuvent être configurés dans le cadre de l'implémentation du Service Cloud ou selon d'autres modalités permises par le Service. Les Données à caractère personnel transférées concernent habituellement les catégories suivantes de données (ou certaines d'entre elles): nom, numéro de téléphone, adresse électronique, fuseau horaire, données liées à l'adresse, données concernant l'accès aux systèmes, les utilisations et autorisations correspondantes, le nom de l'entité légale, données contractuelles, données de facturation et données spécifiques à l'application saisies par les Utilisateurs autorisés du Client dans le Service Cloud, notamment des données liées à des comptes bancaires et cartes de crédit ou de débit.

Catégories de données spéciales (le cas échéant)
Les Données à caractère personnel transférées concernent les catégories spécifiques de données suivantes, telles que définies dans le Formulaire de commande, le cas échéant.

Opérations de traitement
Les Données à caractère personnel transférées sont soumises aux activités de traitement de base suivantes:

- utilisation des Données à caractère personnel pour fournir le Service Cloud (y compris le support technique et opérationnel);
- stockage de Données à caractère personnel dans des Centres de données dédiés (architecture partagée);
- téléchargement de correctifs, mises à jour, montées de version/nouvelles versions sur le Service Cloud;
- sauvegarde de Données à caractère personnel;
- traitement informatique de Données à caractère personnel, notamment la transmission de données, la récupération de données et l'accès aux données;
- accès via un réseau pour permettre le transfert de Données personnelles, si nécessaire.

APPENDICE 2 AU CONTRAT DE TRAITEMENT DE DONNÉES ET AUX CLAUSES CONTRACTUELLES TYPES.

1. PRÉAMBULE

1.1 Dispositions différentes.

Certains Services Cloud font l'objet de conditions de support différentes, spécifiées dans le Supplément ou le Formulaire de commande correspondant.

1.2 Périmètre.

Dans tous les autres cas, la description des mesures de sécurité techniques et organisationnelles définies dans la Section 2 ci-dessous et implémentées par l'Importateur de données pour les Données à caractère personnel conservées dans le système de production du Service Cloud (conformément aux Clauses 4(d) et 5(c) des Clauses contractuelles types) s'applique.

2. MESURES TECHNIQUES ET ORGANISATIONNELLES

Les Sections qui suivent définissent les mesures de sécurité actuelles mises en œuvre par SAP.

2.1 Contrôle des accès physiques.

Les personnes non autorisées ne doivent pas obtenir la permission d'accéder physiquement aux locaux, bâtiments ou salles dans lesquels les systèmes de traitement de données sont situés et qui traitent et/ou utilisent des Données à caractère personnel.

Mesures:

Tous les Centres de données mettent en œuvre des procédures de sécurité strictes, et disposent de gardiens, caméras de surveillance, capteurs de mouvement, mécanismes de contrôle des accès et autres mesures visant à prévenir les intrusions dans les équipements et installations du Centre de données. Seuls des représentants autorisés ont accès aux systèmes et à l'infrastructure présents dans les installations du Centre de données. Pour assurer son bon fonctionnement, l'équipement de sécurité physique (par exemple, les capteurs de mouvement, caméras, etc.) fait l'objet d'un entretien régulier. Les mesures de sécurité physiques qui sont détaillées ci-dessous sont implémentées dans l'ensemble des Centres de données:

(a) SAP protège ses biens et ses installations en recourant aux moyens adaptés, sur la base d'une classification de la sécurité réalisée par un service de sécurité interne.

(b) En règle générale, les bâtiments sont sécurisés par des systèmes de contrôle des accès (système d'accès par carte à puce).

(c) Une exigence minimale impose que l'enveloppe externe du bâtiment soit équipée d'un système certifié de clés incluant une gestion moderne et active des clés.

(d) En fonction de la classification de la sécurité, certains bâtiments, certaines zones précises et leurs environs sont protégés par des mesures supplémentaires. Il peut s'agir notamment de profils d'accès spécifiques, de vidéo-surveillance, de systèmes d'alarme en cas d'intrusion et de systèmes de contrôle d'accès biométriques.

(e) Des droits d'accès seront conférés aux collaborateurs autorisés, au cas par cas, selon le Système et les Mesures de contrôle des accès aux données définies ci-dessous). Cela vaut également pour l'accès des visiteurs. Les invités et visiteurs qui pénètrent dans des locaux de SAP doivent enregistrer leur nom à l'accueil et doivent être accompagnés d'un membre du personnel SAP autorisé. SAP et tous les prestataires tiers de Centres de données consignent les noms et temps de présence des personnes qui pénètrent dans les zones privées de SAP au sein des Centres de données.

(f) Les employés SAP et le personnel extérieur doivent porter leur badge d'identification dans tous les locaux SAP.

2.2 Contrôle des accès au système.

Les systèmes de traitement des données utilisés pour fournir le Service Cloud ne doivent pas pouvoir être utilisés sans autorisation.

Mesures:

(a) Des niveaux d'autorisation multiples sont utilisés pour concéder l'accès aux systèmes sensibles, notamment ceux utilisés pour stocker et traiter les Données à caractère personnel. Des procédures sont en place pour veiller à ce que seuls les utilisateurs autorisés disposent des autorisations requises pour ajouter, supprimer ou modifier des utilisateurs.

(b) Tous les utilisateurs accèdent au système SAP par le biais d'un identifiant propre (identifiant d'utilisateur).

(c) SAP a mis en place des procédures pour faire en sorte que les changements d'autorisation demandés soient mis en œuvre uniquement en accord avec les lignes directrices (par exemple, aucun droit n'est conféré sans autorisation). Si un utilisateur change de rôle ou quitte la société, ses droits d'accès sont révoqués.

(d) SAP a établi une politique en matière de mots de passe qui interdit le partage de mots de passe, impose la marche à suivre en cas de divulgation d'un mot de passe, et exige que les mots de passe soient modifiés périodiquement et les mots de passe par défaut remplacés. Des identifiants d'utilisateur personnalisés sont assignés à des fins d'authentification. Tous les mots de passe doivent être conformes à des exigences minimales définies et sont stockés sous forme chiffrée. Dans le cas des mots de passe de domaine, le système impose un changement tous les six mois et le choix de mots de passe complexes. Chaque ordinateur dispose d'un économiseur d'écran protégé par mot de passe.

(e) Un accès distant à l'environnement de fourniture du Service Cloud requiert au minimum des mécanismes d'authentification complexes (par exemple, la combinaison d'un mot de passe et d'une fonctionnalité de sécurité supplémentaire). Des mots de passe d'une longueur minimale de quinze (15) caractères doivent être utilisés pour les comptes administratifs et les comptes de service des systèmes informatiques pour lesquels la sécurité est primordiale. Le nouveau mot de passe d'un Utilisateur autorisé doit être différent de ses cinq (5) derniers mots de passe. Le réseau de l'entreprise est protégé du réseau public par des pare-feux.

(f) SAP utilise un logiciel antivirus actualisé aux points d'accès au réseau de la société (pour les comptes de messagerie électronique) ainsi que sur l'ensemble des serveurs de fichiers et des postes de travail.

(g) Une gestion des correctifs de sécurité est mise en œuvre pour assurer le déploiement des mises à jour de sécurité pertinentes.

(h) L'accès à distance à l'intégralité du réseau interne de SAP et à son infrastructure critique est protégé par un système d'authentification robuste.

2.3 Contrôle des accès aux données.

Les personnes autorisées à utiliser des systèmes de traitement de données doivent obtenir l'accès uniquement aux Données à caractère personnel auxquelles elles ont le droit. Les Données à caractère personnel ne doivent pas être consultées, copiées, modifiées ou supprimées sans autorisation dans le cadre de leur traitement, utilisation ou stockage.

Mesures:

(a) L'accès aux renseignements personnels, confidentiels ou sensibles est accordé s'il existe un besoin d'accéder auxdites données. En d'autres termes, les employés ou les tiers extérieurs ont accès aux renseignements dont ils ont besoin en vue de s'acquitter de leurs tâches. SAP utilise des concepts d'autorisation qui documentent les procédures d'attribution des

autorisations, et les autorisations qui sont attribuées. Tous les renseignements personnels, confidentiels ou sensibles sont protégés conformément aux normes et politiques de sécurité pertinentes de SAP.

(b) Tous les serveurs de production d'un Service SAP Cloud sont exploités dans les Centres de données/salles de serveurs pertinents. Les mesures de sécurité qui protègent les applications utilisées pour traiter les renseignements personnels, confidentiels ou sensibles sont régulièrement contrôlées. À cette fin, SAP réalise des contrôles de sécurité internes et externes ainsi que des tests de pénétration sur les systèmes informatiques.

(c) SAP n'autorise pas l'installation de logiciels personnels ou autres logiciels non approuvés par SAP dans des systèmes qui sont utilisés pour un Service Cloud.

(d) Une norme de sécurité SAP régit les modalités de suppression ou de destruction des données et des supports de données.

2.4 Contrôle des transmissions de données.

Les Données à caractère personnel ne doivent pas être lues, copiées, modifiées ou supprimées sans autorisation au cours de leur transfert.

Mesures:

(a) Lorsque des supports de données sont transportés physiquement, des mesures adaptées sont mises en œuvre chez SAP pour garantir les niveaux de service convenus (par exemple, chiffrement et conteneurs doublés de plomb).

(b) Les transferts de Données à caractère personnel via les réseaux internes de SAP sont protégés de même que toutes les autres données confidentielles conformément à la Politique de sécurité de SAP.

(c) Lorsque des données sont transférées entre SAP et ses clients, les mesures de protection à appliquer aux Données à caractère personnel transférées sont convenues par les parties dans le Contrat. Cela vaut autant pour un transfert physique que pour un transfert de données via un réseau. Dans tous les cas, le Client assume la responsabilité de tout transfert de données à partir du Point de démarcation de SAP (pare-feu sortant du Centre de données de SAP qui héberge le Service Cloud).

2.5 Contrôle des saisies de données.

Il doit être possible d'examiner et établir rétrospectivement si des Données à caractère personnel ont été saisies, modifiées ou supprimées dans les systèmes de traitement de données utilisés chez SAP pour fournir le Service Cloud, et qui sont les personnes ayant effectué lesdites actions.

Mesures:

L'accès aux Données à caractère personnel est concédé par SAP uniquement aux personnes autorisées, en fonction des besoins pour accomplir leur travail. SAP a mis en œuvre un système de journalisation des saisies, modifications, suppressions et blocages de Données à caractère personnel par SAP ou ses Sous-traitants, dans la plus large mesure autorisée par le Service Cloud.

2.6 Contrôle des tâches.

Les Données à caractère personnel traitées sur commission doivent être traitées conformément au Contrat et aux instructions associées du Client uniquement.

Mesures:

(a) SAP utilise des contrôles et des procédures pour assurer le respect des contrats conclus entre SAP et ses clients, Sous-traitants ou autres prestataires de services.

(b) Dans le cadre de la Politique de sécurité de SAP, les Données client doivent faire l'objet d'un niveau de protection au moins égal à celui des renseignements « confidentiels », conformément à la norme de classification des renseignements de SAP.
(c) Tous les employés et les partenaires contractuels de SAP sont tenus par contrat à respecter la confidentialité de l'ensemble des renseignements sensibles, notamment les secrets commerciaux de clients et partenaires de SAP.

2.7 Contrôle de la disponibilité.

Les Données à caractère personnel doivent être protégées contre la destruction accidentelle ou non autorisée ou la perte.

Mesures:

(a) SAP emploie des procédures de sauvegarde et d'autres mesures visant à assurer une restauration rapide des systèmes essentiels aux activités en cas de besoin.
(b) SAP utilise des systèmes d'alimentation sans coupure (par exemple UPS, batteries, générateurs, etc.) pour garantir l'alimentation continue des Centres de données.
(c) SAP a défini des plans d'intervention d'urgence ainsi que des stratégies de restauration des activités après sinistre pour les Services Cloud.
(d) Les procédures et systèmes d'urgence sont régulièrement mis à l'essai.

2.8 Contrôle de la séparation des données.

Les Données à caractère personnel recueillies à des fins différentes peuvent être traitées séparément.

Mesures:

(a) SAP utilise les capacités techniques des progiciels déployés (par exemple, architecture mutualisée ou environnements système séparés) pour assurer une séparation des données entre les Données à caractère personnel des différents clients.
(b) SAP gère des instances dédiées (avec une séparation logique ou physique) pour chaque Client.
(c) Les Clients (et leurs Sociétés affiliées) ont accès uniquement aux instances propres du Client.

2.9 Contrôle de l'intégrité des données.

Fait en sorte que les Données à caractère personnel demeurent intactes, complètes et actualisées dans le cadre des activités de traitement:

Mesures:

SAP a mis en œuvre une stratégie de défense sur plusieurs niveaux pour garantir une protection contre les modifications non autorisées. Il s'agit des contrôles indiqués dans les rubriques sur les mesures de contrôle qui figurent ci-dessus. Notamment:

(a) Pare-feu
(b) Centre de contrôle de la sécurité
(c) Logiciel antivirus
(d) Sauvegarde et récupération
(e) Tests d'intrusion externe et interne
(f) Vérifications externes régulières pour démontrer la mise en œuvre des mesures de sécurité