CONTRAT DE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL POUR LES SERVICES SAP CLOUD

1. CONTEXTE

1.1 Objectif et application. Le présent document (« **DPA** ») est intégré au Contrat et fait partie d'un accord écrit (y compris au format électronique) conclu entre SAP et le Client. Le présent DPA s'applique aux Données à caractère personnel traitées par SAP et ses Sous-traitants ultérieurs en lien avec la fourniture du Service Cloud. Le présent DPA ne s'applique pas aux environnements non productifs du Service Cloud lorsque ces environnements sont mis à disposition par SAP, et le Client ne doit pas stocker de Données à caractère personnel dans ces environnements.

1.2 Structure. Les Appendices 1 et 2 sont intégrés au présent DPA et en font partie. Ils définissent l'objet convenu, la nature et la finalité du traitement, le type de Données à caractère personnel, les catégories de personnes concernées et les mesures organisationnelles et techniques applicables.

1.3 RGPD. SAP et le Client conviennent qu'il incombe à chaque partie d'examiner et d'adopter les exigences imposées respectivement aux Responsables du traitement et aux Sous-traitants par le Règlement général sur la protection des données 2016/679 (« **RGPD** »), en particulier en ce qui concerne les Articles 28, 32 et 36 du RGPD, si et dans la mesure où cela est applicable aux Données à caractère personnel du Client/des Responsables du traitement qui sont traitées dans le cadre du DPA.

1.4 Gouvernance. SAP agit en qualité de Sous-traitant et le Client ainsi que les entités auxquelles il autorise l'utilisation du Service Cloud agissent en qualité de Responsables du traitement dans le cadre du DPA. Le Client agit en tant que point de contact unique et est seul responsable de l'obtention des autorisations, consentements et permissions nécessaires au traitement des Données à caractère personnel conformément au présent DPA, y compris, le cas échéant, l'approbation des Responsables du traitement pour avoir recours à SAP comme Sous-traitant. Lorsque les autorisations, consentements, instructions ou permissions sont fournis par le Client, ils sont fournis non seulement pour le compte du Client mais aussi pour le compte de tout autre Responsable du traitement qui utilise le Service Cloud. Lorsque SAP informe ou notifie le Client, lesdites informations ou notifications sont réputées reçues par les Responsables du traitement autorisés par le Client à utiliser le Service Cloud. Il incombe au Client de transmettre lesdites informations et notifications aux Responsables du traitement concernés.

2. SECURITE DU TRAITEMENT

2.1 Mesures techniques et organisationnelles appropriées SAP a implémenté et appliquera les mesures organisationnelles et techniques définies dans l'Appendice 2. Le Client a examiné lesdites mesures et convient qu'en ce qui concerne le Service Cloud sélectionné par le Client dans le Bon de commande, les mesures sont appropriées eu égard à l'état de l'art, , aux coûts d'implémentation, à la nature, au périmètre, au contexte et aux objectifs du traitement des Données à caractère personnel.

2.2 Modifications. SAP applique les mesures techniques et organisationnelles définies dans l'Appendice 2 à l'ensemble des clients SAP hébergés sur le même Centre de données et bénéficiant du même Service Cloud. SAP peut modifier les mesures définies dans l'Appendice 2, à tout moment, sans préavis, tant que ces dernières conservent un niveau de sécurité comparable ou renforcé. Les mesures individuelles peuvent être remplacées par de nouvelles mesures ayant la même finalité dès lors qu'elles ne diminuent pas le niveau de sécurité assurant la protection des Données à caractère personnel.

3. OBLIGATIONS DE SAP

3.1 Instructions du Client. SAP ne traitera les Données à caractère personnel que sur instructions documentées du Client. Le Contrat (comprenant le présent DPA) constitue lesdites instructions documentées initiales et chaque utilisation du Service Cloud constitue alors des instructions supplémentaires. SAP mettra en œuvre des efforts raisonnables pour suivre les instructions du Client dès lors qu'elles sont requises par la Loi en matière de protection des données, qu'elles sont techniquement réalisables et qu'elles ne nécessitent pas que des modifications soient apportées au Service Cloud. Si l'une des exceptions mentionnées précédemment s'applique, ou si SAP n'est pas en mesure de respecter une instruction ou estime qu'une instruction enfreint la Loi en matière de protection des données, SAP en informera immédiatement le Client (e-mail autorisé).

3.2 Traitement en application d'une obligation légale. SAP peut également traiter les Données à caractère personnel lorsque la loi applicable l'exige. Dans un tel cas, SAP informera le Client de l'obligation légale préalablement au traitement, sauf si ladite loi interdit une telle information pour des raisons d'intérêt public.

3.3 Personnel. Pour le traitement des Données à caractère personnel, SAP et ses Sous-traitants ultérieurs ne doivent accorder un accès qu'au personnel autorisé et soumis à des obligations de confidentialité. SAP et ses Sous-traitants ultérieurs formeront régulièrement le personnel ayant accès aux Données à caractère personnel aux mesures applicables liées à la sécurité et à la confidentialité des données.

3.4 Coopération. À la demande du Client, SAP coopérera raisonnablement avec le Client et les Responsables du traitement pour répondre aux requêtes émanant de Personnes concernées ou d'une autorité de contrôle concernant le traitement par SAP des Données à caractère personnel ou toute Violation de Données à caractère personnel. SAP est tenu d'informer le Client, dès que cela est raisonnablement possible, de toute demande reçue de la part d'une Personne concernée relative au traitement des Données à caractère personnel, sans répondre à ladite demande en l'absence d'instructions en ce sens du Client. SAP est tenu de fournir une fonctionnalité permettant d'assister le Client dans sa capacité de corriger ou supprimer les Données à caractère personnel du Service Cloud, ou de limiter leur traitement, conformément à la Loi en matière de protection des données. Si ladite fonctionnalité n'est pas fournie, SAP corrigera ou supprimera toute Donnée à caractère personnel, ou limitera leur traitement, conformément aux instructions du Client et à la Loi en matière de protection des données.

3.5 Notification d'une Violation de Données à caractère personnel. SAP notifiera au Client toute Violation de Données à caractère personnel dans les meilleurs délais après en avoir pris connaissance et fournira les informations raisonnables en sa possession pour aider le Client à respecter son obligation de signaler une Violation de Données à caractère personnel, conformément à la Loi en matière de protection des données. SAP peut fournir lesdites informations en plusieurs phases, au fur et à mesure qu'elles seront disponibles. Une telle notification ne saurait être interprétée ou considérée comme une admission de faute ou de responsabilité par SAP.

3.6 Analyse d'impact relative à la protection des données. Si, conformément à la Loi en matière de protection des données, le Client (ou ses Responsables du traitement) est tenu d'effectuer une analyse d'impact relative à la protection des données ou une consultation préalable avec un régulateur, SAP fournira, à la demande du Client, les documents qui sont généralement disponibles pour le Service Cloud (par exemple, le présent DPA, le Contrat, les rapports d'audit ou les certifications). Toute assistance supplémentaire devra être convenue d'un commun accord entre les Parties.

4. EXPORTATION ET SUPPRESSION DES DONNEES

4.1 Exportation et extraction par le Client. Pendant la Durée d'abonnement et conformément au Contrat, le Client peut accéder à ses Données à caractère personnel à tout moment. Le Client

peut exporter et extraire ses Données à caractère personnel dans un format standard. L'exportation et l'extraction peuvent être sujettes à des limitations techniques, auquel cas SAP et le Client détermineront une méthode raisonnable pour permettre au Client d'accéder à ses Données à caractère personnel.

4.2 **Suppression.** Avant l'expiration de la Durée d'abonnement, le Client est autorisé à utiliser les outils d'exportation en libre-service de SAP (s'ils sont disponibles) pour effectuer une exportation finale des Données à caractère personnel depuis le Service Cloud (qui constituera un « renvoi » des Données à caractère personnel). À la fin de la Durée d'abonnement, le Client donne, par les présentes, l'instruction à SAP de supprimer les Données à caractère personnel restantes sur les serveurs qui hébergent le Service Cloud dans un délai raisonnable conformément à la Loi en matière de protection des données (qui ne devra pas dépasser six mois), à moins que la loi applicable n'exige de les conserver.

5. CERTIFICATIONS ET AUDITS

5.1 **Audit client.** Le Client ou un auditeur tiers indépendant raisonnablement acceptable pour SAP (ce qui exclut tout auditeur tiers qui serait un concurrent de SAP ou qui ne disposerait pas des qualifications nécessaires ou d'une indépendance dûment établie) peut auditer l'environnement de contrôle et les pratiques de sécurité de SAP pertinentes au regard du traitement des Données à caractère personnel effectué par SAP seulement si :

- **(a)** SAP n'a pas présenté de justificatifs suffisants attestant de sa conformité aux mesures techniques et organisationnelles qui protègent les systèmes de production du Service Cloud en fournissant : (i) une certification de conformité à la norme ISO 27001 ou à d'autres normes (périmètre défini dans le certificat) ; ou (ii) un rapport d'attestation valide ISAE3402 et/ou ISAE3000, ou bien SOC1-3. Sur demande du Client, les rapports d'audit ou les certifications ISO seront fournis par l'auditeur tiers ou SAP ; ou
- **(b)** Une Violation de Données à caractère personnel s'est produite ; ou
- **(c)** Un audit est requis par l'autorité de contrôle du Client ; ou
- **(d)** La Loi obligatoire en matière de protection des données accorde au Client un droit d'audit direct sous réserve que le Client ne puisse effectuer qu'un seul audit sur une période de douze mois, sauf si la Loi obligatoire en matière de protection des données exige des audits plus fréquents.

5.2 **Audit d'un autre Responsable du traitement.** Un autre Responsable du traitement peut auditer l'environnement de contrôle et les pratiques de sécurité de SAP pertinentes au regard du traitement des Données à caractère personnel effectué par SAP conformément à l'article 5.1 seulement si l'un des cas définis à l'article 5.1 s'applique à cet autre Responsable de traitement. Ledit audit doit être effectué par le Client tel que défini dans l'article 5.1, sauf si la Loi en matière de protection des données exige que l'audit soit effectué par l'autre Responsable du traitement. Si plusieurs Responsables du traitement dont les Données à caractères personnel sont traitées par SAP conformément au Contrat requièrent un audit, le Client doit utiliser tous les moyens raisonnables pour combiner les audits et éviter d'en effectuer plusieurs.

5.3 **Périmètre de l'audit.** Le Client doit fournir un préavis d'au moins soixante jours pour les audits, sauf si la Loi obligatoire en matière de protection des données ou l'autorité de contrôle compétente exige un préavis plus court. La fréquence et le périmètre des audits doivent être convenus d'un commun accord entre les parties agissant raisonnablement et de bonne foi. Les audits du Client ont une durée maximale limitée à trois jours ouvrables. Outre ces restrictions, les parties utiliseront les certifications ou tout autre rapport d'audit en vigueur pour éviter ou minimiser la répétition des audits. Le Client doit fournir les résultats de tout audit à SAP.

5.4 **Coût des audits.** Le Client doit supporter les frais de tout audit, sauf si ledit audit révèle un manquement grave de SAP au présent DPA. Dans ce cas, SAP devra supporter ses propres frais relatifs à l'audit. S'il est établi, suite à un audit, que SAP a manqué à ses obligations en vertu du présent DPA, SAP corrigera promptement ledit manquement à ses propres frais.

6. SOUS-TRAITANTS ULTÉRIEURS

6.1 Utilisation autorisée. Une autorisation générale est accordée à SAP pour sous-traiter le traitement des Données à caractère personnel auprès des Sous-traitants ultérieurs, à condition que :

(a) SAP ou SAP SE agissant pour le compte de SAP recrute les Sous-traitants ultérieurs, au moyen d'un contrat écrit (y compris au format électronique) conforme aux dispositions du présent DPA, concernant le traitement des Données à caractère personnel par le Sous-traitant ultérieur. SAP assume la responsabilité des manquements au Contrat par les Sous-traitants ultérieurs.

(b) SAP évalue les pratiques de sécurité, de protection et de confidentialité d'un Sous-traitant ultérieur préalablement à sa sélection afin d'établir la capacité de ce dernier à offrir le niveau de protection des Données à caractère personnel requis au titre du présent DPA.

(c) La liste des Sous-traitants ultérieurs en place à la date d'entrée en vigueur du Contrat est publiée par SAP ou sera mise à disposition du Client par SAP à sa demande et contiendra le nom, l'adresse et le rôle de chaque Sous-traitant ultérieur auquel SAP a recours pour fournir le Service Cloud.

6.2 Nouveaux Sous-traitants ultérieurs. SAP peut, à son entière discrétion, décider de recourir à de nouveaux Sous-traitants ultérieurssous réserve que :

(a) SAP informe le Client à l'avance (par e-mail ou par message sur le Portail de support disponible via le Support SAP) des ajouts ou remplacements envisagés sur la liste des Sous-traitants ultérieurs comportant le nom, l'adresse et le rôle du nouveau Sous-traitant ultérieur ; et que

(b) Le Client puisse émettre des objections à de telles modifications conformément aux dispositions de l'article 6.3.

6.3 Objections à l'encontre des nouveaux Sous-Traitants ultérieurs.

(a) Si le Client a un motif légitime en vertu de la Loi en matière de protection des données d'émettre une objection à l'encontre du traitement par le nouveau Sous-traitant ultérieur des Données à caractère personnel, le Client peut résilier le Contrat (une telle résiliation étant limitée au Service Cloud sur lequel l'intervention du nouveau Sous-traitant ultérieur est envisagée) par notification écrite à SAP. Ladite résiliation prend effet au moment défini par le Client, étant précisée que cette résiliation ne peut intervenir que dans un délai detrente jours à compter de la date à laquelle SAP a informé le Client du nouveau Sous-traitant ultérieur. Si le Client n'effectue pas de résiliation au cours de ladite période de trente jours, il est réputé avoir accepté le nouveau Sous-traitant ultérieur.

(b) Au cours de ladite période de trente jours à compter de la date à laquelle SAP a informé le Client du nouveau Sous-traitant ultérieur, le Client peut demander à ce que les parties se réunissent pour discuter, de bonne foi, d'une résolution à l'objection émise par le Client. Lesdites discussions ne prolongent pas la période de résiliation et n'affectent pas le droit de SAP d'utiliser le nouveau Sous-traitant ultérieur après la période de trente jours.

(c) Toute résiliation en vertu du présent article 6.3 ne peut être considérée comme un manquement de l'une ou l'autre des parties et est soumise aux conditions du Contrat.

6.4 Remplacement d'urgence. SAP peut remplacer un Sous-traitant ultérieur sans préavis lorsque le motif du changement échappe au contrôle raisonnable de SAP et que le remplacement rapide est justifié pour des raisons de sécurité ou d'urgence. Dans un tel cas, SAP informera le Client du remplacement du Sous-traitant ultérieur le plus rapidement possible suite à sa nomination. L'article 6.3 s'applique en conséquence.

7. TRAITEMENTS INTERNATIONAUX

7.1 Conditions pour les traitements internationaux. SAP est autorisé à traiter les Données à caractère personnel, y compris en ayant recours à des Sous-traitants ultérieurs, conformément

au présent DPA, en dehors du pays dans lequel le Client est situé tel qu'autorisé par Loi en matière de protection des données.

7.2 Clauses contractuelles types. Lorsque (i) les Données à caractère personnel d'un Responsable du traitement situé dans l'EEE ou en Suisse sont traitées dans un pays en dehors de l'EEE, de la Suisse et de tout pays, territoire ou organisation internationale reconnu par l'Union européenne comme assurant un niveau de protection des données adéquat en vertu de l'article 45 du RGPD, ou lorsque (ii) les Données à caractère personnel d'un autre Responsable du traitement sont traitées à l'échelle internationale, et que ledit traitement international nécessite des moyens adéquats en vertu des lois du pays du Responsable du traitement et que les moyens adéquats peuvent être satisfaits en signant les Clauses contractuelles types, alors :

(a) SAP et le Client concluent les Clauses contractuelles types ;

(b) Le Client conclut les Clauses contractuelles types avec chaque Sous-traitant ultérieur concerné, comme suit : soit (i) le Client adhère par les présentes aux Clauses contractuelles types signées par SAP ou SAP SE et le Sous-traitant ultérieur en tant que titulaire indépendant de droits et d'obligations (« Accession Model »), soit (ii) le Sous-traitant ultérieur (représenté par SAP) conclut les Clauses contractuelles types avec le Client (« Power of Attorney Model »). Le Power of Attorney Model s'applique uniquement si et lorsque SAP a expressément confirmé qu'un Sous-traitant ultérieur y est éligible via la liste des Sous-traitants ultérieurs fournie conformément à l'article 6.1(c) ou une notification au Client ; et/ou

(c) Les autres Responsables du traitement autorisés par le Client en vertu du Contrat à utiliser les Services Cloud peuvent également conclure des Clauses contractuelles types avec SAP et/ou les Sous-traitants ultérieurs concernés de la même manière que le Client conformément aux articles 7.2 (a) et (b) ci-dessus. Dans un tel cas, le Client concluera les Clauses contractuelles types pour le compte des autres Responsables du traitement.

7.3 Lien entre les Clauses contractuelles types et le Contrat Rien dans le Contrat ne saurait être interprété comme prévalant sur une clause divergente des Clauses contractuelles types. Afin d'éviter toute incertitude, il est précisé que lorsque le présent DPA prévoit des dispositions supplémentaires sur les règles liées aux audits et aux Sous-traitants ultérieurs dans les articles 5 et 6, de telles dispositions s'appliquent également aux Clauses contractuelles types.

7.4 Droit applicable des Clauses contractuelles types. Les Clauses contractuelles types sont régies par la loi du pays dans lequel le Responsable du traitement concerné est établi.

8. DOCUMENTATION ; REGISTRES DU TRAITEMENT

Chaque partie est tenue de se conformer aux exigences qui lui sont propres en matière de documentation, notamment en ce qui concerne la tenue d'un registre du traitement lorsque la Loi en matière de protection des données l'exige. Chaque partie doit apporter une assistance raisonnable à l'autre partie concernant la mise en œuvre de ses exigences en matière de documentation afin de lui permettre de se conformer à toute obligation liée à la tenue d'un registre du traitement, notamment en fournissant les informations en sa possession dont l'autre partie a besoin et dont elle aura fait la demande par un moyen approprié (via un système électronique par exemple).

9. ACCES UE (OU « EU ACCESS »)

9.1 Services facultatifs. L'Accès UE (ou « EU Access ») est un service facultatif qui peut être proposé par SAP. SAP s'engage alors à fournir le Service Cloud éligible à l'Accès UE, uniquement pour les instances de production dudit Service, conformément aux dispositions du présent article 9. Lorsque l'Accès UE n'a pas été expressément mentionné et convenu dans le Bon de commande pour le Service Cloud qui y est éligible, le présent article 9 ne s'applique pas.

9.2 Accès UE. SAP recourra à des Sous-traitants ultérieurs européens pour toute maintenance nécessitant l'accès aux Données à caractère personnel dans le Service Cloud, et SAP n'exportera pas les Données à caractère personnel en dehors de l'EEE ou de la Suisse, sauf autorisation

expresse du Client par écrit (e-mail autorisé) au cas par cas, ou dans les cas d'exclusion visés à l'article 9.4.

9.3 **Site du centre de données.** À la Date d'entrée en vigueur du Contrat, les Centres de données utilisés pour héberger des Données à caractère personnel dans le Service Cloud sont situés dans l'EEE ou en Suisse. SAP ne migrera pas l'instance Client vers un Centre de données en dehors de l'EEE ou de la Suisse sans l'accord écrit préalable du Client (e-mail autorisé). Si SAP prévoit de migrer l'instance Client vers un Centre de données au sein de l'EEE ou en Suisse, SAP en informera le Client par écrit (e-mail autorisé) au plus tard trente jours avant la migration planifiée.

9.4 **Exclusions.** Les Données à caractère personnel suivantes ne sont pas soumises aux articles 9.2 et 9.3 :

(a) Coordonnées de l'émetteur d'un ticket de maintenance ; et

(b) Toutes autres Données à caractère personnel communiquées par le Client lors de l'émission d'un ticket de maintenance. Le Client peut choisir de ne pas transmettre de Données à caractère personnel lors de l'émission d'un ticket de maintenance. Si de telles données sont nécessaires pour le processus de gestion des incidents, le Client devra anonymiser les Données à caractère personnel préalablement à toute transmission du message d'incident à SAP.

10. DÉFINITIONS

Les termes débutant par une majuscule non définis dans le présent DPA ont la signification qui leur est attribuée dans le Contrat.

10.1 « **Responsable du traitement** » désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des Données à caractère personnel ; dans le cadre du présent DPA, lorsque le Client agit en qualité de sous-traitant pour un autre responsable du traitement, il doit être, vis-à-vis de SAP, considéré comme un Responsable du traitement supplémentaire et indépendant avec les droits et obligations relatifs dont bénéficie un responsable du traitement en application du présent DPA.

10.2 **« 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 Bon de commande.

10.3 « **Loi en matière de protection des données** » désigne la législation applicable protégeant les droits et libertés fondamentaux des personnes et leur droit à la vie privée concernant le traitement des Données à caractère personnel en vertu du Contrat (et comprend, en ce qui concerne la relation entre les parties à l'égard du traitement des Données à caractère personnel par SAP pour le compte du Client, le RGPD comme norme minimale, que les Données à caractère personnel y soient soumises ou non).

10.4 « **Personne concernée** » désigne une personne physique identifiée ou identifiable, telle que définie par la Loi en matière de protection des données.

10.5 **« EEE »** désigne l'Espace économique européen, à savoir les États membres de l'Union européenne avec également l'Islande, le Liechtenstein et la Norvège.

10.6 **« Sous-traitant ultérieur européen »** désigne un Sous-traitant ultérieur qui traite physiquement des Données à caractère personnel dans l'EEE ou en Suisse.

10.7 « **Données à caractère personnel** » désigne les informations se rapportant à une Personne concernée qui sont protégées par la Loi en matière de protection des données. Aux fins du présent DPA, elles comprennent uniquement les données à caractère personnel qui sont (i) saisies par le Client et ses Utilisateurs autorisés dans le Service Cloud ou obtenues via leur utilisation du Service, ou (ii) fournies à ou obtenues par SAP ou ses Sous-traitants ultérieurs en

vue de fournir des services de maintenance conformément au Contrat. Les Données à caractère personnel constituent un sous-ensemble des Données Client (telles que définies dans le Contrat).

10.8 « **Violation de Données à caractère personnel** » désigne (1) la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès d'un tiers non autorisé, de manière accidentelle ou illicite, aux Données à caractère personnel qui soit confirmé(e), ou (2) un incident similaire confirmé impliquant des Données à caractère personnel pour lequel le Responsable du traitement est tenu d'informer les autorités de contrôle compétentes ou les Personnes concernées en vertu de la Loi en matière de protection des données.

10.9 « **Sous-traitant** » désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite les Données à caractère personnel pour le compte du Responsable du traitement, que ce soit de façon directe en tant que Sous-traitant d'un Responsable du traitement ou de façon indirecte en tant que Sous-traitant ultérieur d'un Sous-traitant qui traite les Données à caractère personnel pour le compte du Responsable du traitement.

10.10 **« Clauses contractuelles types »**, parfois également appelées « Clauses du modèle UE », désigne les Clauses contractuelles types (sous-traitants) disponibles sur le lien suivant https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 ou toute version ultérieure publiée par la Commission européenne (laquelle s'appliquera automatiquement).

10.11 « **Sous-traitant ultérieur** » désigne les Sociétés Affiliées de SAP, SAP SE, les Sociétés Affiliées de SAP SE et les tiers engagés par SAP, SAP SE ou les Sociétés Affiliées de SAP SE en relation avec le Service Cloud et qui traitent les Données à caractère personnel conformément au présent DPA.

Appendice 1 au présent DPA et, si applicable, aux Clauses contractuelles types

Exportateur de données
L'Exportateur de données est le Client qui s'est abonné à un Service Cloud qui confère à ses Utilisateurs autorisés le droit de saisir, modifier, utiliser, supprimer ou traiter selon d'autres modalités des Données à caractère personnel. Lorsque le Client autorise d'autres Responsables du traitement à utiliser également le Service Cloud, ces autres Responsables du traitement sont également des Exportateurs de données.

Importateur de données
SAP et ses Sous-traitants ultérieurs fournissent le Service Cloud qui inclut la maintenance suivante :

Les Sociétés Affiliées de SAP SE fournissent la maintenance aux centres de données du Service Cloud à distance depuis des sites de SAP à St. Leon-Rot (Allemagne), en Inde ou depuis d'autres sites où SAP emploie du personnel pour les fonctions Operations/ Cloud Delivery. Les services de maintenance incluent :

- le suivi du Service Cloud ;
- la sauvegarde et la restauration des Données Client conservées dans le Service Cloud ;
- le lancement et le développement de correctifs et de mises à niveau du Service Cloud ;
- le suivi, la correction et l'administration de la base de données et de l'infrastructure sous-jacentes du Service Cloud ;
- la gestion de la sécurité, l'aide à la détection des intrusions réseau, les tests de pénétration.

Les Sociétés Affiliées de SAP SE fournissent également des services de maintenance lorsqu'un Client soumet un ticket de maintenance car le Service Cloud n'est pas disponible ou ne fonctionne pas comme prévu pour plusieurs ou pour tous les Utilisateurs autorisés. SAP fournit une réponse par téléphone, apporte des corrections basiques aux erreurs et gère les tickets de maintenance dans un système de suivi distinct de l'instance de production du Service Cloud.

Personnes concernées
Sauf décision contraire de l'Exportateur de données, les Données à caractère personnel transférées s'appliquent aux catégories de Personnes concernées suivantes : employés, contractuels, Tierces parties d'affaires ou autres individus ayant des Données à caractère personnel 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. Le Client peut configurer les champs de données lors de l'implémentation du Service Cloud ou selon d'autres modalités prévues par le Service Cloud. Les Données à caractère personnel transférées concernent généralement les catégories suivantes de données : 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 la société, données contractuelles, données de facturation et données spécifiques à l'application saisies par les Utilisateurs autorisés dans le Service Cloud qui peuvent inclure des données liées à des comptes bancaires et cartes de crédit ou de débit.

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

Traitement/Finalité

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

- utilisation des Données à caractère personnel pour installer, exploiter, suivre et fournir le Service Cloud (y compris la maintenance technique et opérationnelle) ;
- prestation des Services de conseil ;
- communication avec les Utilisateurs autorisés ;
- stockage de Données à caractère personnel dans des Centres de données dédiés (architecture partagée) ;
- chargement de correctifs ou de mises à niveau du 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 à caractère personnel ;
- exécution des instructions du Client conformément au présent Contrat.

Appendice 2 au présent DPA et, si applicable, aux Clauses contractuelles types – Mesures techniques et organisationnelles

1. MESURES TECHNIQUES ET ORGANISATIONNELLES

Les sections suivantes définissent les mesures techniques et organisationnelles actuelles de SAP. SAP peut les modifier à tout moment sans préavis, tant qu'elles conservent un niveau de sécurité comparable ou renforcé. Les mesures individuelles peuvent être remplacées par de nouvelles mesures ayant la même finalité, sans que ne soit diminué le niveau de sécurité assurant la protection des Données à caractère personnel.

1.1 Contrôle des accès physiques. Les personnes non autorisées ne doivent pas être en mesure d'accéder physiquement aux bâtiments, locaux ou pièces où sont situés les systèmes de traitement de données qui traitent et/ou utilisent les Données à caractère personnel.

Mesures :

- SAP protège ses biens et ses installations en recourant aux moyens adaptés, conformément à la Politique de sécurité de SAP.
- En règle générale, les bâtiments sont sécurisés par des systèmes de contrôle des accès (par exemple, système d'accès par carte à puce).
- Une exigence minimale impose que les points d'entrée externes du bâtiment soient équipés d'un système certifié de clés incluant une gestion moderne et active des clés.
- En fonction de la classification de la sécurité, certains bâtiments, certaines zones précises et leurs environs peuvent être 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.
- Des droits d'accès sont conférés aux collaborateurs autorisés, au cas par cas, selon le Système et les Mesures de contrôle des accès aux données (voir article 1.2 et 1.3 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 autorisé de SAP.
- Les employés SAP et le personnel extérieur doivent porter leur badge d'identification dans tous les locaux SAP.

Mesures supplémentaires pour les Centres de données :

- 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.
- SAP et tous les prestataires tiers de Centres de données consignent les noms et temps de présence du personnel autorisé qui pénètre dans les zones privées de SAP au sein des Centres de données.

1.2 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 :

- Des niveaux d'autorisation multiples sont utilisés lors de la concession de l'accès aux systèmes sensibles, notamment ceux utilisés pour stocker et traiter les Données à caractère personnel. Les autorisations sont gérées par le biais de processus définis conformément à la Politique de sécurité de SAP.

- L'ensemble du personnel accède au système SAP par le biais d'un identifiant propre (identifiant d'utilisateur).
- SAP a mis en place des procédures afin que les changements d'autorisation demandés soient mis en œuvre uniquement en accord avec la Politique de sécurité de SAP (par exemple, aucun droit n'est conféré sans autorisation). Si un membre du personnel quitte la société, ses droits d'accès sont révoqués.
- SAP a établi une politique en matière de mots de passe qui interdit le partage de mots de passe, impose les mesures à prendre 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.
- Le réseau de l'entreprise est protégé du réseau public par des pare-feux.
- 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.
- La gestion des correctifs de sécurité est mise en œuvre pour assurer le déploiement régulier et périodique des mises à jour de sécurité pertinentes. 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.

1.3 Contrôle des accès aux données. Les personnes autorisées à utiliser des systèmes de traitement de données peuvent accéder uniquement aux Données à caractère personnel auxquelles elles ont le droit d'accéder. 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 :

- Dans le cadre de la Politique de sécurité de SAP, les Données à caractère personnel doivent faire l'objet d'un niveau de protection au moins égal à celui des informations « confidentielles », conformément à la norme de classification des informations de SAP.
- L'accès aux Données à caractère personnel est accordé s'il existe un besoin d'accéder auxdites données. Le personnel a accès aux informations dont il a besoin pour pouvoir remplir ses obligations. SAP utilise des concepts d'autorisation qui documentent les processus d'autorisation et les rôles affectés par compte (identifiant d'utilisateur). L'ensemble des Données Client sont protégées conformément à la Politique de sécurité de SAP.
- Tous les serveurs de production sont exploités dans les Centres de données ou des salles de serveurs sécurisées. Les mesures de sécurité qui protègent les applications utilisées pour traiter les Données à caractère personnel sont régulièrement contrôlées. À cette fin, SAP réalise des contrôles de sécurité internes et externes ainsi que des tests de pénétration sur ses systèmes informatiques.
- SAP n'autorise pas l'installation de logiciels qui n’ont pas été approuvés par SAP.
- Une norme de sécurité SAP régit les modalités de suppression ou de destruction des données et des supports de données dès lors qu’ils ne sont plus requis.

1.4 Contrôle des transmissions de données. Excepté en cas de nécessité pour la prestation des Services Cloud conformément au Contrat, les Données à caractère personnel ne doivent pas être consultées, copiées, modifiées ou supprimées sans autorisation pendant leur transfert. 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).

Mesures :

- Les transferts de Données à caractère personnel via les réseaux internes de SAP sont protégés conformément à la Politique de sécurité de SAP.
- 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 et intégrées au Contrat applicable. 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 dès lors qu'il sort du cadre des systèmes contrôlés par SAP (par exemple, données transmises au-delà du pare-feu du Centre de données SAP).

1.5 Contrôle des saisies de données. Il sera 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 SAP et qui sont les personnes ayant effectué lesdites actions.

Mesures :

- L'accès aux Données à caractère personnel est concédé par SAP uniquement au personnel autorisé, en fonction des besoins pour accomplir ses obligations.
- 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 ultérieurs dans le Service Cloud dans la mesure où cela est techniquement possible.

1.6 Contrôle des tâches. Les Données à caractère personnel traitées sur mandat (c'est-à-dire, les Données à caractère personnel traitées pour le compte du client) sont traitées conformément au Contrat et aux instructions associées du Client uniquement.

Mesures :

- SAP utilise des contrôles et des procédures pour assurer le respect des contrats conclus entre SAP et ses clients, sous-traitants ultérieurs ou autres prestataires de services.
- Dans le cadre de la Politique de sécurité de SAP, les Données à caractère personnel doivent faire l'objet d'un niveau de protection au moins égal à celui des informations « confidentielles », conformément à la norme de classification des informations de SAP.
- Tous les employés et les sous-traitants ultérieurs contractuels ou autres prestataires de services sont tenus par contrat à respecter la confidentialité de l'ensemble des informations sensibles, notamment les secrets commerciaux de clients et partenaires de SAP.

1.7 Contrôle de la disponibilité. Les Données à caractère personnel seront protégées contre les destructions accidentelles ou non autorisées et contre les risques de perte.

Mesures :

- SAP emploie des procédures de sauvegarde régulières visant à assurer une restauration des systèmes essentiels aux activités en cas de besoin.
- SAP utilise des systèmes d'alimentation sans coupure (par exemple UPS, batteries, générateurs, etc.) pour garantir l'alimentation continue des Centres de données.
- SAP a défini des plans d'intervention d'urgence pour les processus de gestion critiques et peut proposer des stratégies de restauration après sinistre pour les Services critiques, tels que définis plus en détail dans la Documentation ou intégrés au Bon de commande du Service Cloud applicable.
- Les procédures et systèmes d'urgence sont régulièrement mis à l'essai.

1.8 Contrôle de la séparation des données. Les Données à caractère personnel recueillies à des fins différentes peuvent être traitées séparément.

Mesures :

- 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 provenant de différents clients.
- Le Client (et ses Responsables du traitement) ont accès uniquement à leurs propres données.
- Si des Données à caractère personnel sont requises pour la gestion d'un incident de maintenance émanant du Client, les données sont affectées audit message afin de traiter ledit message. Il est impossible d'y accéder afin de traiter un autre message. Lesdites données sont stockées dans des systèmes d'aide dédiés.

1.9 Contrôle de l'intégrité des données. 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.

SAP utilise les éléments suivants pour mettre en œuvre les articles relatifs aux contrôles et aux mesures décrits précédemment, Notamment :

- Pare-feu
- Centre de contrôle de la sécurité
- Logiciel antivirus
- Sauvegarde et récupération
- Tests d'intrusion externe et interne
- Audits externes réguliers pour démontrer la mise en œuvre des mesures de sécurité