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

## 1. CONTEXTE

### 1.1 Objet.

Le présent document est un contrat de traitement des données (le « **DPA** ») conclu entre SAP et le Client, et s'applique aux Données à caractère personnel fournies par le Client et chaque Responsable du traitement dans le cadre de leur utilisation du Service Cloud. Il précise les mesures techniques et organisationnelles que SAP utilise pour protéger les Données à caractère personnel qui sont conservées dans le système de production du Service Cloud.

### 1.2 Application du document Clauses contractuelles types.

Si le traitement des Données à caractère personnel implique un Transfert international, les Clauses contractuelles types s'appliquent en vertu de l'article 5 et sont intégrées par référence.

### 1.3 Gouvernance.

Sauf indication contraire en vertu de l'article 5.2, le Client est le seul responsable de l'administration de toutes les demandes émanant d'autres Responsables du traitement. Le Client exigera des autres Responsables du traitement autorisés à utiliser le Service Cloud qu'ils respectent les conditions du présent DPA.

## 2. APPENDICES

Le Client et ses Responsables du traitement établissent la/les finalité(s) de la collecte et du traitement des Données à caractère personnel dans le cadre du Service Cloud. L'Appendice 1 précise les détails du traitement que fournira SAP via le Service Cloud. L'Appendice 2 précise les mesures techniques et organisationnelles que SAP applique au Service Cloud, sauf indication contraire dans le Contrat.

## 3. OBLIGATIONS DE SAP

### 3.1 Instructions du Client.

SAP suivra les instructions reçues de la part du Client (pour son propre compte ou pour le compte de ses Responsables de traitement) à l'égard des Données à caractère personnel, sauf si elles (i) font l'objet d'une interdiction légale ou (ii) nécessitent l'apport de modifications substantielles au Services Cloud. SAP peut corriger ou supprimer toute Donnée à caractère personnel, conformément à l'instruction du Client. Si SAP n'est pas en mesure de respecter une instruction, SAP en informera le Client dans les meilleurs délais (une communication par e-mail est autorisée).

### 3.2 Secret des données.

Pour le traitement de Données à caractère personnel, SAP et ses Sous-traitants ultérieurs ne recourront qu'à des collaborateurs s'étant engagés à respecter le secret des données et des télécommunications en vertu de la Loi en matière de protection des données. SAP et ses Sous-traitants ultérieurs formeront régulièrement les collaborateurs ayant accès aux Données à caractère personnel aux mesures liées à la sécurité et à la confidentialité des données.

### 3.3 Mesures techniques et organisationnelles.

**(a)** SAP recourra aux mesures techniques et organisationnelles appropriées définies dans l'Appendice 2.

**(b)** L'Appendice 2 s'applique au système de production du Service Cloud. Le Client ne doit pas conserver des Données à caractère personnel dans des environnements non productifs.

**(c)** SAP fournit le Service Cloud à l'ensemble des clients SAP hébergés sur le même centre de données et bénéficiant du même Service Cloud. Le Client reconnaît que SAP pourra améliorer les mesures prises dans le cadre de l'Appendice 2 pour la protection des Données à caractère personnel, tant que le niveau de protection des données n'en est pas diminué.

### 3.4 Notification d'une violation de la sécurité.

SAP informera le Client dans les meilleurs délais dès que SAP prend connaissance d'une Violation de la sécurité.

**3.5 Coopération.**

À la demande du Client, SAP apportera une assistance raisonnable au Client ou aux autres Responsables du traitement pour répondre aux requêtes émanant de Personnes concernées ou d'une autorité de réglementation à l'égard du traitement de Données à caractère personnel par SAP.

## 4. SOUS-TRAITANTS ULTÉRIEURS

**4.1 Utilisation autorisée.**

**(a)** Le Client et les Responsables du traitement autorisent SAP à confier le traitement des Données à caractère personnel à des Sous-traitants ultérieurs. SAP assume la responsabilité de tout manquement au Contrat par ses Sous-traitants.

**(b)** Les Sous-traitants s'acquitteront des mêmes obligations que SAP en tant que Sous-traitant initial (ou Sous-traitant ultérieur) à l'égard du traitement des Données à caractère personnel.

**(c)** SAP évaluera les pratiques de sécurité, de protection et de confidentialité d'un Sous-traitant ultérieur avant de le sélectionner. Les Sous-traitants ultérieurs peuvent être titulaires de certifications de sécurité attestant qu'ils recourent à des mesures de sécurité appropriées. Si tel n'est pas le cas, SAP évaluera régulièrement les pratiques de sécurité qui sont liées au traitement des données de chaque Sous-traitant.

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

**4.2 Nouveaux Sous-traitants ultérieurs.**

SAP décide à son entière discrétion de recourir à des Sous-traitants ultérieurs, à condition que :

**(a)** SAP informe le Client à l'avance (par e-mail ou par message sur le Portail de support) de toute modification affectant la liste des Sous-traitants ultérieurs en place à la Date d'entrée en vigueur (sauf dans le cas de Remplacements d'urgence ou de suppressions de Sous-traitants ultérieurs sans remplacement).

**(b)** Si le Client a un motif valable lié au traitement de Données à caractère personnel par les Sous-traitants ultérieurs, le Client peut s'opposer au recours par SAP à un Sous-traitant ultérieur, en informant SAP par écrit dans les trente jours qui suivent la réception de l'avis de SAP. Si le Client s'oppose au recours d'un Sous-traitant ultérieur, les parties se réuniront de bonne foi pour négocier une résolution. SAP peut choisir : (i) de ne pas recourir au Sous-traitant ultérieur ou (ii) de prendre les mesures correctives demandées par le Client dans son objection puis recourir au Sous-traitant ultérieur. Si aucune des présentes options ne peut raisonnablement être choisie et que le Client maintient son objection pour un motif légitime, chacune des parties est autorisée à résilier le Contrat moyennant un préavis écrit de trente jours. Si le Client ne fait pas objection dans les trente jours qui suivent la réception de l'avis, le Client est réputé avoir accepté le nouveau Sous-traitant ultérieur.

**(c)** Si l'objection du Client n'est pas résolue dans les soixante jours qui suivent son dépôt et que SAP n'a pas reçu de préavis de résiliation, le Client est réputé accepter le Sous-traitant ultérieur.

**4.3 Remplacement d'urgence.**

SAP peut changer de Sous-traitant ultérieur lorsque le motif du changement échappe au contrôle raisonnable de SAP. Dans un tel cas, SAP informera le Client du remplacement du Sous-traitant ultérieur le plus rapidement possible. Le Client se réserve le droit de faire objection au remplacement du Sous-traitant ultérieur en vertu de l'article 4.2(b).

## 5. TRANSFERTS INTERNATIONAUX

**5.1 Limitations concernant le transfert international.**

Les Données à caractère personnel émanant d'un/de Responsable(s) du traitement situé(s) dans l'EEE ou en Suisse ne doivent pas être exportées par SAP ou ses Sous-traitants ultérieurs en dehors de l'EEE ou de la Suisse (un **« Transfert international »**), à moins de respecter les conditions suivantes :

**(a)** le destinataire ou le pays ou territoire depuis lequel il traite ou accède aux Données à caractère personnel garantit un niveau de protection adéquat des droits et libertés des Personnes concernées en rapport avec le traitement des Données à caractère personnel, tel que déterminé par la Commission Européenne ; ou

**(b)** en vertu des exigences visées à l'article 5.2.

**5.2 Clauses contractuelles types et cadre multi-niveaux.**

**(a)** Les Clauses contractuelles types s'appliquent dans le cadre d'un Transfert international vers un pays qui ne garantit pas un niveau de protection adéquat des droits et libertés des Personnes concernées en rapport avec le traitement des Données à caractère personnel, tel que déterminé par la Commission Européenne.

**(b)** SAP a conclu avec les Sous-traitants ultérieurs d'un pays tiers la version non modifiée des Clauses contractuelles types avant le traitement des Données à caractère personnel par lesdits Sous-traitants ultérieurs. Le Client (pour lui-même et pour le compte de chaque Responsable du traitement) adhère par les présentes aux Clauses contractuelles types conclues entre SAP et le Sous-traitant ultérieur d'un pays tiers. SAP fera valoir les Clauses contractuelles types à l'encontre du Sous-traitant ultérieur pour le compte du Responsable de traitement si un droit d'application directe n'est pas disponible en vertu de la Loi en matière de protection des données.

**(c)** Rien dans le présent DPA ne saurait être interprété comme prévalant sur une clause divergente des Clauses contractuelles types.

## 6. CERTIFICATIONS ET AUDITS

**6.1 Audits client.**

Le Client ou un auditeur tiers indépendant peut auditer l'environnement de contrôle et les pratiques de sécurité de SAP pertinentes relativement aux Données à caractère personnel traitées par SAP, uniquement 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 et à d'autres normes (périmètre défini dans le certificat) ; ou (ii) un rapport d'attestation valide ISAE3402 et/ou ISAE3000. Sur demande du Client, l'auditeur tiers ou SAP devra fournir les rapports d'audit SOC (relatifs aux contrôles des sociétés de services) et les certifications ISO.

**(b)** Une Violation de la sécurité s'est produite.

**(c)** Le Client ou un autre Responsable du traitement a des motifs raisonnables de suspecter que SAP manque à ses obligations en vertu du présent DPA.

**(d)** Un audit est requis par l'autorité de protection des données du Client ou d'un autre Responsable du traitement.

**(e)** La Loi obligatoire en matière de protection des données accorde au Client un droit d'audit direct.

Lorsque le Client audite l'environnement de SAP, SAP apportera une assistance raisonnable au Client dans ses processus d'audit.

**6.2 Restrictions relatives à l'audit.**

Le Client ne pourra effectuer, sur une période de douze mois, qu'un seul audit dont la durée maximale sera limitée à 3 jours ouvrables et dont le périmètre sera convenu à l'avance entre les parties. Un préavis doit être fourni dans un délai raisonnable d'au moins soixante jours, sauf si la Loi en matière de protection des données exige la réalisation de l'audit à une date antérieure. SAP et le Client utiliseront les certifications actuelles et des rapports d'autres audits pour minimiser la répétition des audits. Le Client et SAP assumeront chacun leurs propres frais relatifs à l'audit, à moins que le Client procède à un audit en vertu de l'article 6.1 (c) (sauf si ledit audit révèle une violation commise par SAP, auquel cas SAP devra assumer ses propres frais relatifs à l'audit), 6.1 (d) ou 6.1 (e). Dans de tels cas, le Client assumera ses propres frais ainsi que le coût pour les collaborateurs internes de

SAP requis pour conduire l'audit. S'il est établi, suite à un audit, que SAP a manqué à ses obligations en vertu du présent Contrat, SAP corrigera la violation immédiatement et à ses propres frais.

## 7. ACCÈS UE

### 7.1 Services facultatifs.

Si le Bon de commande l'indique, SAP accepte de fournir un Accès UE au Service Cloud éligible en vertu de l'article 7.

### 7.2 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.

### 7.3 Site du centre de données.

À la Date d'entrée en vigueur du Bon de commande, 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.

### 7.4 Exclusions.

Les Données à caractère personnel suivantes ne sont pas soumises aux exigences stipulées dans les articles 7.2 et 7.3 :

**(a)** Coordonnées de l'auteur d'une demande de maintenance ;

**(b)** Toutes autres Données à caractère personnel envoyées par le Client lors du dépôt d'une demande de maintenance. Le Client peut choisir de ne pas transmettre les Données à caractère personnel lors du dépôt d'une demande de maintenance. Si lesdites données sont nécessaires pour le processus de gestion des incidents, le Client devra rendre anonymes lesdites Données à caractère personnel préalablement à toute transmission du message d'incident à SAP ;

**(c)** Données à caractère personnel dans des systèmes non productifs.

## 8. DÉFINITIONS

Les termes débutant par une majuscule non définis dans les présentes ont la signification qui leur est affectée dans le Contrat.

**8.1** Le terme **« 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.

**8.2** Le terme **« Responsable du traitement »** désigne une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui, seul(e) ou associé(e) à d'autres personnes, détermine les finalités et les méthodes de traitement des Données à caractère personnel.

**8.3** Le terme **« Sous-traitant initial »** désigne une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui traite les données à caractère personnel pour le compte du responsable.

**8.4** Le terme **« 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.

**8.5** Le terme **« Personne concernée »** désigne une personne physique identifiée ou identifiable.

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

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

**8.8** Le terme **« Données à caractère personnel »** désigne toute information liée à une Personne concernée aux fins du présent DPA et 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 Cloud. Sont comprises également les données à caractère personnel fournies à ou obtenues par SAP ou ses Sous-traitants ultérieurs en vue de fournir des services de maintenance en vertu du Contrat. Les Données à caractère personnel constituent un sous-ensemble de Données Client.

**8.9** Le terme **« Violation de la sécurité »** désigne (1) la destruction, la perte, l'altération ou la divulgation accidentelle ou illégale de Données à caractère personnel ou de Données confidentielles du Client, ou (2) un incident similaire impliquant des Données à caractère personnel pour lequel le Responsable du traitement est tenu d'informer la Personne concernée en vertu de la loi applicable.

**8.10** Le terme **« Clauses contractuelles types »**, parfois également appelé « Clauses du modèle UE », désigne les (Clauses contractuelles types (sous-traitants)) ou toute version ultérieure qui en est publiée par la Commission (laquelle s'appliquera automatiquement). Les Clauses contractuelles types actuellement en vigueur sont disponibles à l'adresse http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc. Elles comprennent les Appendices 1 et 2 joints au présent DPA.

**8.11** Le terme **« Sous-traitant ultérieur »** désigne les Sociétés Affiliées de SAP et les tiers engagés par SAP ou par des Sociétés Affiliées de SAP pour traiter des données à caractère personnel.

**8.12** Le terme **« Sous-traitant ultérieur d'un pays tiers »** désigne tout Sous-traitant ultérieur constitué en personne morale en dehors de l'EEE ou d'un 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.

**Appendice 1 au Contrat de traitement de données et aux Clauses contractuelles types**

**Exportateur de données**
L'Exportateur de données 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.

**Importateur de données**
SAP et ses Sous-traitants ultérieurs fournissent le Service Cloud, ce qui inclut la maintenance suivante :
Les Sociétés Affiliées de SAP apportent leur soutien 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 la fonction Opérations/Services Cloud). 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 fournissent également une maintenance lorsqu'un Client soumet une demande 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 demandes 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 suivantes, telles que définies dans le Bon 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 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 : Mesures techniques et organisationnelles

### 1. MESURES TECHNIQUES ET ORGANISATIONNELLES

Les articles qui suivent définissent les mesures de sécurité actuelles mises en œuvre par SAP. SAP peut les modifier à tout moment sans préavis, tant qu'elles conservent un niveau de sécurité comparable ou renforcé. De ce fait, il est possible que des mesures individuelles soient remplacées par de nouvelles mesures ayant la même finalité, sans diminuer le niveau de sécurité assuré.

### 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, sur la base d'une classification de la sécurité réalisée par un service de sécurité interne.
- 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 des personnes qui pénètrent 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 les Services SAP 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. Des procédures sont en place pour veiller à ce que les utilisateurs autorisés disposent des autorisations requises afin d'ajouter, supprimer ou modifier des utilisateurs.
- Tous les utilisateurs accèdent 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 les lignes directrices (par exemple, aucun droit

n'est conféré sans autorisation). Si un utilisateur 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 informations personnelles, confidentielles 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 informations 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 personnes auxquelles les autorisations sont attribuées. Toutes les informations personnelles, confidentielles ou sensibles sont protégées conformément aux normes et politiques de sécurité pertinentes de SAP. Les informations confidentielles doivent être traitées dans le respect de leur confidentialité.
- 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 informations personnelles, confidentielles ou sensibles 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 personnels ou autres 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 conformément au contrat de services pertinent, les données à caractère personnel ne pas doivent être consultées, copiées, modifiées ou supprimées 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).

- Les transferts de Données à caractère personnel via les réseaux internes de SAP sont protégés de la même manière que toutes les autres données confidentielles 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. 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 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 ultérieurs, dans toute la mesure permise par les Produits et les Services de SAP.

**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.
- Pour les services de maintenance sur site, SAP fournit une installation sécurisée spécialement conçue pour la prise en charge des demandes de maintenance, dans laquelle SAP met à disposition une zone de sécurité surveillée à accès contrôlé pour transférer les mots de passe et les données d'accès. Les clients SAP ont à tout moment le contrôle de leurs connexions de maintenance à distance. Les employés de SAP ne peuvent accéder à un système client sans que le client en question n'en soit informé et ne participe activement à cette fin.

**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 et d'autres mesures visant à assurer une restauration rapide 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 ainsi que des stratégies de restauration des activités après sinistre pour les Services fournis.
- 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.
- Les Clients (et leurs Sociétés Affiliées) ont accès uniquement à leurs propres données.
- Si des Données à caractère personnel sont requises pour la gestion d'un incident de maintenance émanant d'un client spécifique, 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