CONTRAT DE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL POUR LES SERVICES DE SUPPORT ET PROFESSIONNELS SAP

1. CONTEXTE

1.1 Objectif et application. Le présent document (« **DPA** ») est intégré au Contrat et fait partie d'un contrat écrit (y compris au format électronique) conclu entre SAP et le Client. Le présent DPA s'applique aux Données à caractère personnel fournies par le Client et chaque Responsable du traitement dans le cadre de l'exécution des services SAP définis dans le Contrat applicable (le ou les « Service(s) SAP ») auquel le présent DPA est joint, notamment:

(a) Les services de Support SAP définis dans le Contrat de licence et de support; et/ou

(b) Les Services professionnels décrits dans le contrat de services conclu entre SAP et le Client (le « Contrat de services »).

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 l'objectif du traitement, le type de Données à caractère personnel, les catégories de données, les 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 aux Responsables du traitement et Sous-traitants ultérieurs 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 applicable aux Données à caractère personnel du Client/des Responsables du traitement qui sont traitées dans le cadre du DPA. À titre d'exemple, l'Appendice 3 répertorie les exigences applicables du RGPD et les Sections correspondantes du présent DPA.

1.4 Gouvernance. SAP agit en qualité de Sous-traitant et Client, et les entités qu'il autorise à inclure des Données à caractère personnel dans les systèmes accessibles par SAP lors de l'exécution du Service SAP agissent en qualité de Responsables du traitement dans le cadre du DPA. Le Client sert de point de contact unique et c'est à lui qu'incombe exclusivement l'obtention des autorisations et consentements nécessaires pour le 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, instructions ou consentements 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. Lorsque SAP informe ou notifie le Client, lesdits renseignements ou notifications sont réputés reçus par les Responsables du traitement autorisés par le Client à inclure les Données à caractère personnel. Il incombe au Client de transmettre lesdits renseignements et notifications aux Responsables du traitement concernés.

2. SÉCURITÉ 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 que les mesures sont appropriées et tiennent compte de la technologie, des coûts de l'implémentation, de la nature, du périmètre, du contexte et des objectifs du traitement des Données à caractère personnel.

L'Appendice 2 s'applique uniquement dans la mesure où lesdits Services SAP sont exécutés sur ou à partir d'un site SAP. Si SAP exécute les Services SAP sur le site du Client et qu'il a accès aux systèmes et données du Client, SAP doit alors se conformer aux conditions administratives, techniques et physiques raisonnables du Client pour sécuriser lesdites données et les protéger contre tout accès non autorisé. Dans le cadre d'un accès aux systèmes et données du Client, le Client est chargé de fournir au personnel de SAP les autorisations et mots de passe utilisateur pour accéder à ses systèmes et annuler lesdites autorisations et résilier ledit accès, lorsqu'il le jugera pertinent le cas échéant. Le Client n'accorde pas à SAP l'accès aux systèmes ou

renseignements personnels (du Client ou de tout tiers) sauf si ledit accès est essentiel pour l'exécution des Services SAP. Le Client ne doit pas conserver des Données à caractère personnel dans des environnements non productifs.

2.2 Modifications. SAP applique les mesures techniques et organisationnelles définies dans l'Appendice 2 à l'ensemble des clients SAP bénéficiant du même Service SAP. SAP peut modifier les mesures définies dans l'Appendice 2 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 diminuer le niveau de sécurité assurant la protection des Données à caractère personnel.

3. OBLIGATIONS DE SAP

3.1 Instructions du Client. SAP traitera les Données à caractère personnel exclusivement selon les instructions fournies par le Client. Le Contrat (comprenant le présent DPA), constitue lesdites instructions initiales fournies. Le Client peut fournir des instructions supplémentaires pendant l'exécution du Service SAP. SAP mettra en œuvre des efforts raisonnables pour suivre les instructions du Client, du moment qu'elles sont requises par la Loi en matière de protection des données, qu'elles sont techniquement faisables et qu'elles ne nécessitent aucune modification au niveau de l'exécution du Service SAP. 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 informera immédiatement le Client (courriel autorisé).

3.2 Traitement conforme aux obligations juridiques. SAP peut également traiter les Données à caractère personnel lorsque la loi applicable l'exige. Dans un tel cas, SAP informera le Client des obligations juridiques préalablement au traitement, sauf si ladite loi interdit de tels renseignements pour des raisons d'intérêt public.

3.3 Personnel. Pour traiter les Données à caractère personnel, SAP et ses Sous-traitants ultérieurs doivent uniquement accorder un accès au personnel autorisé qui s'est engagé à respecter la 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 réglementation à l'égard du traitement des Données à caractère personnel par SAP ou de toute Violation des Données à caractère personnel. SAP est tenu d'informer le Client dès que raisonnablement possible des demandes reçues de la part d'une Personne concernée en rapport avec le traitement des Données à caractère personnel, sans répondre lui-même à ladite demande avant d'avoir obtenu des instructions supplémentaire du Client, le cas échéant. SAP corrigera ou supprimera les Données à caractère personnel en sa possession (le cas échéant), ou limitera leur traitement, conformément à l'instruction du Client et à la Loi en matière de protection des données.

3.5 Notification d'une Violation des Données à caractère personnel. À compter de la découverte d'une Violation des Données à caractère personnel, SAP en informera le Client dans les meilleurs délais et fournira les renseignements raisonnables en sa possession pour aider le Client à respecter son obligation de signaler une Violation des Données à caractère personnel, conformément à la Loi en matière de protection des données. SAP peut fournir lesdits renseignements en plusieurs phases, au fur et à mesure qu'ils sont mis à disposition. 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 SAP (par exemple, le présent DPA, le Contrat, les rapports de vérification ou les certifications). Une assistance supplémentaire doit être convenue d'un commun accord entre les Parties.

4. SUPPRESSION DES DONNÉES

Le Client donne l'ordre à SAP par les présentes de supprimer les Données à caractère personnel restant en sa possession (le cas échéant) dans un délai raisonnable, conformément à la Loi en matière de protection des données (sans dépasser six mois) dès lors qu'elles ne sont plus requises aux fins de la signature du Contrat, à moins que la loi applicable n'exige de les conserver.

5. CERTIFICATIONS ET VÉRIFICATIONS

5.1 Vérification client. Le Client ou son vérificateur tiers indépendant convenant à SAP (qui ne doit pas inclure de vérificateur tiers qui soit un concurrent de SAP, qui ne dispose pas des qualifications nécessaires, ou dont le statut d'indépendant n'a pas été dûment reconnu) peut effectuer une vérification des centres d'exécution des services et de support et des pratiques de sécurité de SAP relativement aux Données à caractère personnel traitées par SAP, seulement si:

- **(a)** SAP n'a pas présenté de justificatifs suffisants attestant de sa conformité aux mesures techniques et organisationnelles en fournissant une certification de conformité à la norme ISO 27001 et à d'autres normes (périmètre défini dans le certificat). Les certifications sont disponibles à l'adresse: https://www.sap.com/corporate/en/company/quality.html#certificates ou, si ce n'est pas le cas, sur demande.
- **(b)** Une Violation des Données à caractère personnel s'est produite.
- **(c)** Une vérification est requise par l'autorité de protection des données du Client.
- **(d)** La Loi obligatoire en matière de protection des données accorde au Client un droit de vérification direct à condition que le Client effectue une seule vérification sur une période de douze mois, sauf si la Loi obligatoire en matière de protection des données exige des vérifications plus fréquentes.

5.2 Vérification d'un autre Responsable du traitement. Un autre Responsable du traitement peut effectuer des vérifications de l'environnement de contrôle et des pratiques de sécurité de SAP relativement aux Données à caractère personnel traitées par SAP, conformément à la Section 5.1 seulement si l'un des cas définis à la Section 5.1 s'applique à un autre Responsable du traitement. Ladite vérification doit être effectuée par le Client tel que défini dans la Section 5.1, sauf si la vérification doit être effectuée par l'autre Responsable du traitement lui-même conformément à la Loi en matière de protection des données. Si plusieurs Responsables du traitement dont les Données à caractères personnel sont traitées par SAP conformément au Contrat requièrent une vérification, le Client doit utiliser tous les moyens raisonnables pour combiner les vérifications et éviter d'en effectuer plusieurs.

5.3 Périmètre de la vérification. Le Client doit fournir un préavis d'au moins soixante jours pour les vérifications, sauf si la Loi obligatoire en matière de protection des données ou une autorité de protection des données compétente exige un préavis plus court. La fréquence, les délais et le périmètre des vérifications doivent être convenus d'un commun accord entre les parties qui agissent de manière raisonnable et de bonne foi. Les audits des Clients sont limités à des audits à distance, dans la mesure du possible. Si un audit sur site est requis, il ne pourra pas excéder un jour ouvrable. Au-delà desdites restrictions, les parties utiliseront les certifications actuelles ou les rapports d'autres de vérification pour éviter ou minimiser la répétition des vérifications. Le Client doit fournir les résultats des vérifications à SAP.

5.4 Coût des vérifications. Le Client doit assumer les frais de la vérification, sauf si ladite vérification révèle un manquement substantiel de SAP au présent DPA. Dans ce cas, SAP devra

assumer ses propres frais relatifs à la vérification. S'il est établi, suite à une vérification, que SAP a manqué à ses obligations en vertu du présent DPA, SAP corrigera le manquement immédiatement et 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 pour son compte engage les Sous-traitants ultérieurs dans le cadre d'un contrat écrit (y compris au format électronique), conformément aux conditions du présent DPA en rapport avec le traitement des Données à caractère personnel par le Sous-traitant ultérieur. SAP sera tenu responsable des violations par le Sous-traitant ultérieur, conformément aux conditions du Contrat.

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

(c) S'agissant du Support SAP, la liste des Sous-traitants ultérieurs établie par SAP en place à la date d'entrée en vigueur du Contrat soit publiée par SAP (sous https://support.sap.com/en/my-support/subprocessors.html) ou que SAP la mette à disposition du Client à la demande, y compris le nom, l'adresse et le rôle de chaque Sous-traitant ultérieur auquel SAP a recours pour fournir le Service SAP.

(d) S'agissant des Services professionnels, SAP mette, à la demande du Client, la liste à disposition ou qu'il identifie lesdits Sous-traitants ultérieurs avant le début des Services SAP concernés.

6.2 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 des ajouts ou remplacements souhaités sur la liste des Sous-traitants ultérieurs, y compris le nom, l'adresse et le rôle du nouveau Sous-traitant ultérieur (i) dans le cadre du Support SAP, par le biais d'une publication sur le SAP Support Portal, ou par e-mail, lors de l'enregistrement du Client sur le portail SAP et (ii) dans le cadre des Services professionnels, par le biais d'une publication similaire sur le SAP Support Portal, ou par courriel, ou sous toute autre forme écrite.

(b) Le Client puisse s'opposer à de telles modifications, tel que défini dans la Section 6.3.

6.3 Oppositions aux nouveaux Sous-Traitants ultérieurs.

(a) Support SAP: si le Client a un motif valable en vertu de la Loi en matière de protection des données de s'opposer au traitement par le nouveau Sous-traitant ultérieur des Données à caractère personnel, le Client peut résilier le Support SAP sur notification écrite adressée à SAP, ladite notification devant être envoyée à SAP au plus tard trente jours après la date à laquelle SAP informe le Client du nouveau Sous-traitant ultérieur. Si le Client ne notifie pas SAP de son intention de résilier le Support SAP au cours de ladite période de trente jours, il est réputé avoir accepté le nouveau Sous-traitant ultérieur. Au cours de ladite période de trente jours à compter de la date à laquelle SAP informe le Client du nouveau Sous-traitant ultérieur, le Client peut demander à ce que les parties se réunissent de bonne foi pour négocier une résolution à l'opposition. Lesdites négociations ne prolongent pas la période de préavis de résiliation et n'affectent pas le droit de SAP d'utiliser le nouveau Sous-traitant ultérieur après la période de trente jours.

(b) Services professionnels: si le Client a un motif valable en vertu de la Loi en matière de protection des données lié au traitement des 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 cinq jours ouvrables qui suivent la réception de l'avis de SAP décrit à la Section 6.2. 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 les services concernés moyennant un préavis écrit de cinq jours. Si le Client ne fait pas objection dans les cinq jours qui suivent la réception de l'avis, le Client est réputé avoir accepté le Sous-traitant ultérieur. Si l'objection du Client n'est pas résolue dans les trente jours qui suivent son dépôt et que SAP n'a pas reçu de préavis de résiliation, le Client est réputé avoir accepté le Sous-traitant ultérieur.

(c) Toute résiliation en vertu de la présente Section 6.3 ne doit pas être considérée comme étant une faute de l'une ou l'autre des parties et doit être 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 requis 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. La Section 6.3 s'applique en conséquence.

7. TRAITEMENT INTERNATIONAL

7.1 Conditions pour le traitement international. 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 la 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 d'un pays, organisation ou territoire reconnu par l'Union européenne comme un pays qui assure un niveau adéquat de protection des données en vertu de l'Art. 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 moyen adéquats peuvent être satisfaits en signant les Clauses contractuelles types, alors:

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

(b) Le Client signe les Clauses contractuelle types avec chaque Sous-traitant ultérieur concerné, comme suit: soit (i) le Client adhère aux Clauses contractuelles types signées par SAP ou SAP SE et le Sous-traitant ultérieur en tant titulaire indépendant de droits et d'obligations (« Modèle d'adhésion »), soit (ii) le Sous-traitant ultérieur (représenté par SAP) signe les Clauses contractuelles types avec le Client (« Modèle de procuration »). Le modèle de procuration s'applique uniquement si et lorsque SAP a confirmé qu'un Sous-traitant ultérieur y est éligible via la liste des Sous-traitants ultérieurs fournie conformément à la Section 6.1(c) ou en informant le Client.

(c) Et/Ou les autres Responsables du traitement autorisés par le Client à inclure des Données à caractère personnel en vertu du Contrat peuvent également signer des Clauses contractuelles types avec SAP et/ou les Sous-traitants ultérieurs concernés de la même manière que le Client conformément aux Sections 7.2 (a) et (b) ci-dessus. Dans un tel cas, le Client signera 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 présent Contrat ne saurait être interprété comme prévalant sur une clause divergente des Clauses contractuelles types. Pour ne laisser subsister aucun doute, lorsque le présent DPA apporte davantage de

spécifications sur les règles liées aux vérifications et Sous-traitants ultérieurs dans les Sections 5 et 6, lesdites spécifications s'appliquent en relation 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; ENREGISTREMENTS DU TRAITEMENT

Chaque partie est tenue de se conformer aux exigences en matière de documentation qui lui sont propres, notamment la gestion des enregistrements 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 ses exigences en matière de documentation, y compris fournir les renseignements dont elle a besoin et de la façon dont elle a raisonnablement fait la demande (via un système électronique par exemple) afin que l'autre partie soit en mesure de respecter toute obligation relative à la gestion des enregistrements du traitement.

9. DÉFINITIONS

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

9.1 Le terme « **Utilisateurs autorisés** » désigne toute personne physique à qui le Client donne l'autorisation d'utiliser le Service SAP dans le cadre d'une licence de progiciel SAP et qui est un employé, un agent, un prestataire ou un représentant (i) du Client, (ii) des Sociétés affiliées du Client, et/ou (iii) d'un Partenaire d'affaires du Client et de ses Sociétés affiliées (tels que définis dans le Contrat de licence et de support).

9.2 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; aux fins du présent DPA, lorsque le Client agit en qualité de sous-traitant pour un autre responsable du traitement, il doit, en relation avec SAP, être considéré comme un Responsable du traitement supplémentaire et indépendant qui dispose des droits et obligations relatifs aux responsables du traitement en vertu du présent DPA.

9.3 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 (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).

9.4 Le terme « **Personne concernée** » désigne une personne physique identifiée ou identifiable, tel que défini par la Loi en matière de protection des données.

9.5 Le terme « **Données à caractère personnel** » désigne les renseignements relatifs à une Personne concernée qui sont protégés par la Loi en matière de protection des données. Pour les besoins du présent DPA, il inclut uniquement les données à caractère personnel fournies à ou accessibles par SAP ou ses Sous-traitants ultérieurs aux fins de l'exécution du Service SAP dans le cadre du Contrat.

9.6 Le terme « **Violation des 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 façon accidentelle ou illégale, aux Données à caractère personnel, ou (2) un incident similaire impliquant des Données à caractère personnel pour lequel le Responsable du traitement est tenu d'informer les autorités de protection des données compétentes ou les Personnes concernées en vertu de la Loi en matière de protection des données.

9.7 Le terme « **Services professionnels** » désigne les services d'implémentation, les services de conseil et/ou les services tels que les Services de support SAP Premium Engagement, les

Services de développement de solutions de gestion innovantes et les Services de support de développement de solutions de gestion innovantes.

9.8 Le terme « **Sous-traitant** » 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 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.

9.9 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 européenne (laquelle s'appliquera automatiquement).

9.10 Le terme « **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 SAP et qui traitent les Données à caractère personnel conformément au présent DPA.

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

Exportateur de données
L'Exportateur de données désigne le Client ayant conclu un Contrat de licence et de support et/ou un Contrat de services avec SAP en vue de l'acquisition du Service SAP décrit dans le Contrat applicable. L'Exportateur de données autorise les autres Responsables du traitement à utiliser également le Service SAP; lesdits autres Responsables du traitement sont aussi des Exportateurs de données.

Importateur de données
SAP et ses Sous-traitants ultérieurs fournissent le Service SAP tel que défini dans le Contrat applicable conclu avec l'Exportateur de données, lequel inclut notamment le Service SAP suivant:

- S'agissant du Contrat de licence et de support: SAP et/ou ses Sous-traitants ultérieurs fournissent un support lorsqu'un Client soumet une demande de support car le Progiciel n'est pas disponible ou ne fonctionne pas comme prévu. Ils fournissent une réponse par téléphone, apportent des corrections basiques aux erreurs et gèrent les messages de support dans un système de suivi.
- S'agissant du Contrat de services spécifique aux Services professionnels: SAP et/ou ses Sous-traitants ultérieurs fournissent les Services régis par le Formulaire de commande et le Périmètre des Services correspondant.

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, prestataires, partenaires d'affaires ou autres individus ayant des Données à caractère personnel transmises à, mises à la disposition de ou obtenues par l'Importateur de données.

Catégories de données
Les Données à caractère personnel transférées concernent les catégories de données suivantes:

Le Client détermine les catégories de données et/ou les champs de données pouvant être transféré(e)s par Service SAP tel qu'indiqué dans le Contrat applicable. Les Données à caractère personnel transférées concernent généralement les catégories de données suivantes: nom, numéro de téléphone, adresse électronique, fuseau horaire, données liées à l'adresse, données concernant l'accès aux systèmes, les utilisations et autorisations correspondantes, nom de la société, données contractuelles, données de facturation et données spécifiques à l'application transférées par les Utilisateurs autorisés qui peuvent inclure des données financières telles que 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 Contrat (y compris le Formulaire de commande), le cas échéant.

Objectifs/Opérations de traitement
Les Données à caractère personnel transférées sont soumises aux activités de traitement de base définies dans le Contrat, notamment:

- utilisation des Données à caractère personnel pour fournir le Service SAP;
- stockage des Données à caractère personnel;
- traitement informatique de Données à caractère personnel pour la transmission de données;
- exécution des instructions du Client conformément au présent Contrat.

Appendice 2 au 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 diminuer 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 Sections 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 SAP autorisé.
- 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 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. 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 courriel) 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 renseignements « confidentiels », conformément à la norme de classification des renseignements 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 renseignements 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 SAP conformément au Contrat pertinent, 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 requises pour le transfert des données sont convenues par les présentes par SAP et son client 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 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. Le contrôle des tâches est nécessaire et permet de garantir que les Données à caractère personnel traitées pour le compte d'autrui le sont conformément aux instructions du Client.

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 renseignements « confidentiels », conformément à la norme de classification des renseignements 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 renseignements sensibles, notamment les secrets commerciaux de clients et partenaires de SAP.

  S'agissant du Support SAP, les clients SAP ont à tout moment le contrôle de leurs connexions de support à distance. Les employés de SAP ne peuvent accéder à un système client sans que le client en question n'en soit informé et n'y consente. Pour le Support SAP, SAP fournit une installation sécurisée spécialement conçue pour la prise en charge des demandes de support, 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 support à distance. Les employés de SAP ne peuvent accéder à un système client sur site 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 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 de continuité des activités pour les processus de gestion critiques.
- 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 des commandes techniques appropriées pour assurer une séparation des Données à tout moment.
- Le Client (et ses Responsables du traitement approuvés) a accès à ses propres Données uniquement, grâce à une authentification sécurisée et à des autorisations.
- Si des Données à caractère personnel sont requises pour la gestion d'un incident de support 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 Sections relatives 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
- Vérifications externes régulières pour démontrer la mise en œuvre des mesures de sécurité

Appendice 3 au DPA

Le tableau suivant définit les Articles applicables du RGPD et les termes correspondants au DPA, à titre d'exemple uniquement.

Article du RGPD	**Section du DPA**	**Cliquez sur le lien pour accéder à la Section**
28(1)	2 et Appendice 2	Sécurité du traitement et Appendice 2, Mesures techniques et organisationnelles.
28(2), 28(3) (d) et 28 (4)	6	Sous-traitants ultérieurs.
28 (3), première phrase	**Error! Reference source not found.** et Appendice 1, 1.2	Objectif et application. Structure**.**.
28(3) (a) et 29	3.1 et 3.2	Instructions du Client. Traitement conforme aux obligations juridiques.
28(3) (b)	3.3	Personnel.
28(3) (c) et 32	2 et Appendice 2	Sécurité du traitement et Appendice 2, Mesures techniques et organisationnelles.
28(3) (e)	3.4	Coopération.
28(3) (f) et 32-36	2 et Appendice 2, 3.5, 3.6	Sécurité du traitement et Appendice 2, Mesures techniques et organisationnelles. Notification d'une Viloation des Données à caractèere personnel. Analyse d'impact relative à la protection des données.
28(3) (g)	4	Suppression des données.
28(3) (h)	5	CERTIFICATIONS ET VÉRIFICATIONS.
28 (4)	6	Sous-traitants ultérieurs.
30	8	Documentation; enregistrements du traitement.
46(2) (c)	7.2	Clauses contractuelles types.