

Conditions relatives à la Protection des Données à caractère personnel

Juillet 2021

Les Conditions relatives à la Protection des Données à caractère personnel ("**CPD**") sont convenues entre l'entité Siemens ("**Siemens**") et le Client ("**Client**") nommés dans l'Accord.

1. Cadre et conformité aux lois

1.1. Les CPD s'appliquent au Traitement des Données à caractère personnel par Siemens agissant en tant que Sous-traitant du Client en ce qui concerne les Offres prévues par l'Accord. Dans l'Accord, l'Offre telle que définie dans le présent document peut être désignée par le terme "Service". Les Annexes des CPD font partie intégrante des CPD. Les CPD font partie intégrante de l'Accord ; en cas de conflit, les Annexes des CPD prévalent sur les CPD qui prévaut sur le reste de l'Accord.

1.2. Les CPD décrivent les droits et obligations du Client et de Siemens en matière de protection des données dans le cadre des opérations de traitement concernées par les CPD. Tous les autres droits et obligations sont exclusivement régis par les autres parties de l'Accord.

1.3. Lorsqu'elle fournit les Offres, Siemens se conforme aux lois et règlements sur la protection des données directement applicables à la fourniture des Services en tant que Sous-traitant du Client, y compris la loi sur la notification des violations de sécurité. Toutefois, Siemens n'est pas responsable du respect de la conformité aux lois ou réglementations en matière de protection des données applicables au Client ou au secteur d'activité du Client qui ne sont pas généralement applicables aux Sous-traitants. Le Client doit se conformer à toutes les lois et réglementations applicables à l'usage des Offres par les Clients, y compris la Législation applicable en matière de protection des données, et s'assurer que Siemens et son Sous-traitant ultérieur sont autorisés à fournir les Services décrits dans les CPD.

2. Détails du traitement

Les détails des opérations de Traitement fournis par Siemens, y compris l'objet du Traitement, la nature et la finalité du Traitement, les types de Données à caractère personnel traitées et les catégories de Personnes concernées affectées, sont précisés dans les Annexes des CPD.

3. Instructions

Siemens ne traitera les Données à caractère personnel que conformément aux instructions écrites du Client. Le Client convient que l'Accord (y compris les CPD) constitue les instructions écrites du Client à Siemens pour le Traitement des Données à caractère personnel. Toute instruction supplémentaire ou alternative doit être convenue par écrit entre les parties.

4. Mesures techniques et organisationnelles

4.1. Compte tenu de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque de probabilité et de gravité variables des droits et libertés des personnes physiques, Siemens met en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque. Les mesures techniques et organisationnelles mises en œuvre par Siemens à cette fin sont décrites dans les Annexes des CPD. Le Client comprend et

accepte que les mesures techniques et organisationnelles sont soumises au progrès et au développement technique. À cet égard, Siemens se réserve le droit de mettre en œuvre des mesures de substitution adéquates tant que le niveau de sécurité des mesures est maintenu.

4.2. Les mesures techniques et organisationnelles décrites dans les Annexes des CPD s'appliquent au système informatique et aux applications de Siemens et de ses Sous-traitants ultérieurs. Le Client est responsable de la mise en œuvre et du maintien de mesures techniques et organisationnelles adéquates pour les composants qu'il fournit ou contrôle, comme la mise en œuvre de mesures de contrôle d'accès physique et de système pour ses propres locaux, actifs et systèmes informatiques ou la configuration des Offres en fonction des besoins individuels du Client.

5. Confidentialité du traitement

Siemens veillera à ce que le personnel chargé du Traitement des Données à caractère personnel (i) soit tenu de préserver la confidentialité de ces données, (ii) traite ces données uniquement de la manière décrite dans les CPD ou selon les instructions écrites du Client, et (iii) reçoive une formation adéquate en matière de confidentialité et de sécurité.

6. Sous-traitants ultérieurs

6.1. Le Client approuve par la présente l'engagement de Sous-traitants ultérieurs par Siemens. Une liste à jour des Sous-traitants ultérieurs mandatés par Siemens est disponible dans les Annexes pertinentes des CPD.

6.2. Siemens se réserve le droit de supprimer ou d'ajouter à tout moment de nouveaux Sous-traitants ultérieurs. Si la Législation applicable en matière de protection des données l'exige, Siemens obtiendra l'approbation du Client pour engager de nouveaux Sous-traitants ultérieurs conformément à la procédure suivante : (i) Siemens informe le Client au moins 30 jours à l'avance avant d'autoriser un nouveau Sous-traitant ultérieur à accéder aux Données à caractère personnel du Client ; (ii) si le Client n'adresse pas d'objections raisonnables comprenant une explication des motifs de non-approbation par écrit dans ce délai de 30 jours, l'absence d'objection a valeur d'approbation du nouveau Sous-traitant ultérieur ; (iii) si le Client adresse des objections raisonnables, Siemens s'efforcera, avant d'autoriser le Sous-traitant ultérieur à accéder aux Données à caractère personnel, de a) recommander une modification de la configuration ou de l'utilisation des Offres par le Client afin d'éviter le Traitement des Données à caractère personnel par le nouveau Sous-traitant ultérieur visé par l'objection ou b) proposer d'autres mesures qui répondent aux préoccupations soulevées dans l'objection du Client ; (iv) si les modifications ou les mesures proposées ne peuvent pas éliminer les motifs de non-approbation, le Client peut résilier l'Offre concernée sans pénalité avec un préavis écrit de 14 jours maximum après la réponse de

Siemens à l'objection du Client. Si le Client ne résilie pas l'Offre concernée dans le délai de 14 jours, cette absence de résiliation a valeur d'approbation du Sous-traitant ultérieur par le Client.

6.3 En cas de recours à des Sous-traitants ultérieurs, Siemens conclut avec ces derniers un contrat imposant au Sous-traitant ultérieur des obligations contractuelles appropriées qui ne sont pas moins protectrices que les obligations des présentes CPD. Siemens demeure responsable des actes ou omissions de ses Sous-traitants ultérieurs de la même manière que de ses propres actes et omissions en vertu des présentes.

7. Transferts vers des bénéficiaires hors de l'EEE

7.1. Dans le cas où les Transferts vers des Destinataires hors de l'EEE concernent des Données à caractère personnel provenant d'un Responsable du traitement situé dans l'EEE, en Suisse ou au Royaume-Uni, Siemens mettra en œuvre les Garanties de Transfert définies dans les Annexes des CPD. Siemens se réserve le droit de remplacer la Garantie de transfert définies dans les Annexes des CPD par d'autres Garanties de Transfert adéquates. Dans ce cas, le mécanisme de notification et d'objection défini de la Section 6.2 s'applique mutatis mutandis.

7.2. Les dispositions suivantes s'appliquent si une Garantie de Transfert est basée sur les Clauses contractuelles types :

(i) Siemens, si elle est située en dehors de l'EEE ou d'un pays ayant pris une Décision d'Adéquation, et le Client concluent par les présentes les Clauses contractuelles types. Le Client conclut les Clauses contractuelles types en son nom et pour son propre compte et pour le compte et au nom de ses Responsables du traitement Supplémentaires. Les "Annexe des CPD - Description des Opérations de Traitement" et "Annexes des CPD - Mesures techniques et organisationnelles" constituent les annexes 1 et 2 des Clauses contractuelles types.

(ii) Siemens conclut les Clauses contractuelles types avec ses Sous-traitants ultérieurs situés hors de l'EEE ou d'un pays faisant l'objet d'une Décision d'Adéquation. Les Clauses contractuelles types couvrent les activités de Traitement fournies par le Sous-traitant ultérieur concerné. Le Client et les autres Responsables du traitement deviennent un exportateur de données en vertu des Clauses contractuelles types comme suit : a) les Clauses contractuelles types prévoient le droit pour le Client et les autres Responsables du traitement d'adhérer aux Clauses contractuelles types par déclaration unilatérale, c'est-à-dire que les Clauses contractuelles types lient le Client, les autres Responsables du traitement et le Sous-traitant ultérieur concerné dès que le Client déclare son adhésion (et indépendamment de la réception de la déclaration par Siemens ou le Sous-traitant ultérieur) ("**Mécanisme d'Adhésion**") ; ou b) Siemens conclut les Clauses contractuelles types avec le Sous-traitant ultérieur pour le compte du Client et des autres Responsables du traitement ("**Mécanisme de Mandat**"). Le Mécanisme de Mandat s'applique si Siemens a confirmé dans les Annexes des CPD qu'un Sous-traitant ultérieur y est éligible.

(iii) Les parties savent que la Commission de l'Union européenne a publié un nouveau jeu de clauses contractuelles types conformément à la décision d'exécution de la Commission (UE) 2021/914 à compter du 4 juin 2021 (" Clauses contractuelles types (UE) 2021/914 "). Siemens remplacera les Clauses Contractuelles Types par les nouvelles Clauses Contractuelles Types (UE) 2021/914 avant le 27

septembre 2021 par Siemens, (a) si elle est située en dehors de l'EEE ou d'un pays ayant pris une décision d'adéquation, en concluant les modules 2 et 3 des Clauses Contractuelles Types (UE) 2021/914 avec le Client, ou (b) si elle est située dans l'EEE ou dans un pays ayant pris une décision d'adéquation, en concluant le module 3 des Clauses Contractuelles Types (UE) 2021/914 avec le Sous-traitant respectif.

7.3. Les dispositions suivantes s'appliquent si une Protection de Transfert est basée sur les BCR-P : Siemens oblige contractuellement ce Sous-traitant ultérieur à respecter les Règles d'entreprises contraignantes des Sous-traitants ultérieurs en ce qui concerne les Données à caractère personnel traitées dans le cadre des présentes CPD.

7.4. Engagement supplémentaire de Siemens : Outre les engagements pris dans le cadre des Garanties de Transfert, Siemens confirme qu'elle n'a aucune raison de croire que la législation qui lui est applicable ou qui est applicable à ses Sous-traitants ultérieurs, y compris dans tout pays vers lequel des Données à caractère personnel sont transférées soit par elle, soit par l'intermédiaire d'un Sous-traitant ultérieur, l'empêche de respecter les instructions reçues du Client et ses obligations au titre des CPD ou des Garanties de Transfert et qu'en cas de modification de cette législation susceptible d'avoir un effet défavorable substantiel sur les engagements et obligations prévus par les présentes CPD ou les Garanties de Transfert, elle notifiera rapidement cette modification au Client dès qu'elle en aura connaissance, auquel cas le Client est en droit de suspendre le transfert des Données à caractère personnel et/ou de résilier l'Accord.

8. Défense des Données à caractère personnel des Clients - Demandes d'accès par des tiers

Si Siemens reçoit d'un tiers une demande de divulgation de Données à caractère personnel, Siemens (i) s'efforcera, dans la mesure du raisonnable, de rediriger le tiers vers le Client pour lui adresser directement sa demande de données ; (ii) en informera rapidement le Client, à moins que la législation en vigueur ne l'interdise, et, s'il lui est interdit d'informer le Client, s'efforcera, dans la mesure du possible, d'obtenir le droit de lever l'interdiction afin de communiquer le plus d'informations possible au Client ; et (iii) s'efforcera, dans la mesure du raisonnable, de contester la demande de divulgation en invoquant des lacunes juridiques dans la législation du demandeur ou des conflits avec la législation de l'EEE ou de l'État membre de l'EEE

9. Violation des Données à caractère personnel

9.1. Siemens notifie le Client sans délai après avoir eu connaissance d'une Violation des Données à caractère personnel. En fonction de la nature du traitement et des informations dont dispose Siemens, la notification décrit (i) la nature de la Violation de Données à caractère personnel, y compris, dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées et les catégories et le nombre approximatif d'enregistrements de Données à caractère personnel concernés, (ii) un contact auprès duquel des informations supplémentaires peuvent être obtenues, (iii) les conséquences probables de la Violation de Données à caractère personnel et (iv) les mesures prises ou envisagées pour remédier à la Violation de Données à caractère personnel. Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations simultanément, celles-ci peuvent être fournies par étapes sans retard excessif.

9.2. Siemens (i) aidera dans la mesure du raisonnable le Client en se conformant à ses obligations en matière de Violation de Données à caractère personnel conformément à la Législation applicable en matière de protection des données, et (ii) prendra les mesures correctives appropriées et raisonnables.

10. Droits des personnes concernées, assistance de Siemens

10.1. Dans la mesure où la loi l'autorise, Siemens notifie le Client sans délai si elle reçoit une demande d'une Personne concernée à exercer ses droits (tels que le droit d'accès, de rectification, d'effacement ou de restriction du Traitement).

10.2. En fonction de la nature du traitement et des informations dont dispose Siemens, (i) Siemens assistera le Client par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour l'exécution de l'obligation du Client de répondre aux demandes d'exercice des droits de la Personne concernée ; (ii) à sa propre discrétion, soit a) fournira au Client la possibilité de rectifier ou d'effacer les Données à caractère personnel via les fonctionnalités des Offres, soit (ii) rectifiera ou effacera les Données à caractère personnel selon les instructions du Client ; et (iii) aidera raisonnablement le Client en se conformant à ses autres obligations en vertu de la Législation applicable en matière de protection des données. Toute assistance supplémentaire au titre du point (iii) doit faire l'objet d'un accord mutuel entre les parties.

11. Audits

11.1. Sous réserve qu'un droit d'audit soit requis par la Législation applicable en matière de protection des données, le Client a le droit de vérifier, par des moyens appropriés, conformément aux Sections 11.2 à 11.4 ci-dessous, le respect par Siemens et ses Sous-traitants ultérieurs des obligations en matière de protection des données prévues par les présentes annuellement, à moins que des audits supplémentaires ne soient nécessaires en vertu de la Législation applicable en matière de protection des données. Ces audits seront limités aux systèmes d'information et de traitement des données qui sont pertinents pour la fourniture des Offres fournies au Client.

11.2. Siemens et ses Sous-traitants ultérieurs peuvent faire appel à des auditeurs (internes ou externes) afin de réaliser des audits visant à vérifier le respect des obligations en matière de protection des données prévues par les présentes. Chaque audit donnera lieu à la production d'un rapport d'audit ("**Rapport d'Audit**"). À la demande du Client, Siemens fournit les Rapports d'Audit pertinents pour les Offres concernées. Le Client accepte que ces Rapports d'Audit soient avant tout utilisés pour traiter les droits d'audit du Client en vertu des CPD.

11.3. Si la Législation applicable en matière de protection des données l'exige, Siemens autorisera des audits supplémentaires, y compris des audits sur site dans les installations et locaux de Siemens par le Client ou une société d'audit tierce indépendante et accréditée, pendant les heures de bureau, moyennant un préavis raisonnable à Siemens. Le Client est responsable de tous les coûts et frais liés à cet audit supplémentaire.

11.4. Les Rapports d'Audit et toute autre information et documentation fournie au cours d'un audit constituent des informations confidentielles et ne peuvent être fournis aux autres Responsables du traitement qu'en vertu d'obligations de

confidentialité substantiellement équivalentes aux obligations de confidentialité contenues ailleurs dans l'Accord. Si les audits portent sur des Sous-traitants ultérieurs, Siemens peut exiger du Client et des autres Responsables du traitement qu'ils concluent des accords de non-divulgence directement avec le Sous-traitant ultérieur concerné avant de remettre les Rapports d'Audit et toute autre information ou documentation au Client ou aux autres Responsables du traitement.

12. Point de contact unique et responsabilité

12.1. Le Client sert de point de contact unique pour Siemens, également pour les autres Responsables du traitement dans le cadre des CPD.

12.2. Dans le cas où les CPD ou l'une des Garanties de Transfert visées à la Section 7 (telles que les Clauses contractuelles types) confèrent des droits aux Responsables du traitement (y compris les Responsables du traitement autres que le Client) à l'égard de Siemens et/ou de ses Sous-traitants ultérieurs, le Client est tenu, sauf disposition contraire du droit applicable en matière de protection des données, d'exercer ces droits en contactant directement Siemens, en son nom propre et/ou au nom du Responsable du traitement concerné. Siemens et ses Sous-traitants ultérieurs sont en droit de refuser toute demande, instruction ou réclamation émanant directement d'un Responsable du traitement autre que le Client.

12.3. Dans le cas où les CPD ou l'une des Garanties de Transfert contient des obligations de notification à l'égard des Responsables du traitement, Siemens est libérée de son obligation de notification à un Responsable du traitement lorsque Siemens a fourni cette notification au Client, à moins que la Législation applicable en matière de protection des données n'en dispose autrement.

12.4. Sans préjudice des droits prévus par la loi des Personnes concernées, les limitations de responsabilité contenues dans l'Accord s'appliquent également à la responsabilité de Siemens et de ses Sous-traitants ultérieurs (pris dans leur ensemble) vis-à-vis du Client et de ses autres Responsables du traitement.

12.5. Le Client est tenu de veiller à ce que les Sections 12.1 à 12.4 ci-dessus soient applicables par Siemens et ses Sous-traitants ultérieurs vis-à-vis de ses autres Responsables du traitement.

13. Notifications

13.1. Siemens peut notifier le Client en vertu des CPD en publiant une notification telle que décrite dans l'Accord.

13.2. Les notifications concernant les Sous-traitants ultérieurs en vertu de la Section 6 des CPD peuvent être diffusées en dressant la liste des Sous-traitants actuels à l'adresse suivante www.siemens.com/dpt et en fournissant au Client un mécanisme pour obtenir la notification de tout nouveau Sous-traitant ultérieur. Le Client a l'obligation d'enregistrer un point de contact pour recevoir les notifications relatives aux Sous-traitants ultérieurs à l'adresse suivante www.siemens.com/dpt et de tenir à jour ses coordonnées pour les notifications.

14. Durée et résiliation

Les CPD ont la même durée que l'Accord. À la fin des CPD et sauf accord contraire entre les parties dans l'Accord, Siemens efface toutes les Données à caractère personnel mises à sa disposition ou obtenues ou générées par Siemens pour le compte du Client dans le cadre des Offres.

15. Langue

Si Siemens fournit une traduction de la version anglaise des CPD ou de ses annexes, la version anglaise des CPD ou de ses annexes prévaut en cas de conflit.

16. Conditions spécifiques au pays

16.1. Fédération de Russie Si Siemens traite des Données à caractère personnel dans le cadre de la loi sur la protection des données n° 152 FZ (i) le Client est responsable de la collecte initiale, de l'enregistrement, de la systématisation, du stockage, de la mise à jour, de la modification, du transfert et de l'extraction (collectivement "**Traitement initial**") de ces Données à caractère personnel ; et (ii) le Client déclare par la présente qu'il effectuera le Traitement initial conformément à la législation relative au traitement et à la protection de ces informations. Le Client déclare avoir obtenu le consentement de la Personne concernée relatif au transfert (y compris le transfert international) et le Traitement de ses Données à caractère personnel par Siemens et ses Sous-traitants ultérieurs.

16.2. États-Unis Si Siemens traite des Données à caractère personnel de résidents américains, Siemens prend les engagements supplémentaires suivants envers le Client : Siemens traitera les Données à caractère personnel pour le compte du Client et ne conservera, n'utilisera ni ne divulguera ces Données à caractère personnel à d'autres fins que celles énoncées dans les CPD et dans les limites autorisées par la loi américaine sur la confidentialité des données ("**US Data Privacy Law**"), y compris en vertu d'une exemption de "vente". En aucun cas, le Client ne vendra (tel que ce terme est défini dans la loi américaine sur la confidentialité des données) ces Données à caractère personnel. Ces conditions supplémentaires ne limitent ni ne réduisent les engagements de Siemens en matière de protection des données pris envers le Client dans les CPD, le contrat ou tout autre accord entre Siemens et le Client. Siemens certifie par la présente qu'elle comprend les restrictions contenues dans le présent document et qu'elle s'y conformera.

17. Définitions

17.1. "**Accord**" désigne l'accord commercial relatif à la fourniture des Offres entre Siemens et le Client.

17.2. "**Législation applicable en matière de protection des données**" signifie toute loi applicable relative au Traitement des Données à caractère personnel en vertu des présentes.

17.3. "**Règles d'entreprise contraignantes pour les Sous-traitants**" ou "**BCR-P**" désigne les Règles d'entreprise contraignantes pour les Sous-traitants approuvées conformément à l'Article 47 du règlement général sur la protection des données (UE) 2016/679.

"**Responsable du traitement**" désigne la personne physique ou morale qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement des Données à caractère personnel.

17.4. "**Pays faisant l'objet d'une décision d'adéquation**" désigne un pays situé en dehors de l'EEE où la Commission européenne a décidé que le pays assure un niveau de protection adéquat en ce qui concerne les Données à caractère personnel.

17.5. "**Personne concernée**" désigne une personne physique identifiée ou identifiable.

17.6. "**CPD**" désigne les présentes Conditions relatives à la Protection des Données à caractère personnel.

17.7. "**Annexes des CPD**" désigne les documents qui décrivent le champ d'application, la nature et la finalité du Traitement, les types de Données à caractère personnel traitées, les catégories de Personnes concernées, les Sous-traitants ultérieurs utilisés et les mesures techniques et organisationnelles, et qui sont référencés dans l'Accord et/ou les CPD.

17.8. "**EEE**" désigne l'Espace économique européen.

17.9. "**Autre Responsable du traitement**" désigne tout tiers (tel qu'une société affiliée du Client) agissant en tant que Responsable du traitement qui est habilité à utiliser ou à recevoir des Offres en vertu des termes de l'Accord.

17.10. "**Offres**" désigne les Offres prévues par l'Accord et fournies par Siemens en sa qualité de Sous-traitant. Dans l'Accord, l'Offre telle que définie dans le présent document peut être désignée par le terme "Service".

17.11. "**Données à caractère personnel**" désigne les informations qui se rapportent, directement ou indirectement, à une Personne concernée, y compris, sans limitation, les noms, les adresses électroniques, les adresses postales, les numéros d'identification, les données de localisation, les identifiants en ligne ou un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne. Les Données à caractère personnel, aux fins des CPD, comprennent uniquement les Données à caractère personnel transmises par ou pour le Client ou tout autre Responsable du traitement dans le cadre des Offres ou celles auxquelles Siemens a accès dans le cadre de la fourniture des Offres.

17.12. "**Violation de Données à caractère personnel**" désigne une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des Données à caractère personnel traitées selon les termes des présentes CPD.

17. "**Sous-traitant**" désigne une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui traite des Données à caractère personnel pour le compte d'un Responsable du traitement.

17.13. "**Traiter**" ou "**Traitement**" désigne toute opération ou ensemble d'opérations effectuées sur des Données à caractère personnel ou des ensembles de Données à caractère personnel, par des moyens automatisés ou non, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre mise à disposition, le rapprochement ou la combinaison, la restriction, l'effacement ou la destruction, l'accès, le transfert et l'élimination.

17.14. "**Clauses contractuelles types**" désigne les Clauses contractuelles types pour le transfert de Données à caractère personnel à des Sous-traitants établis dans des pays tiers conformément à la décision 2010/87/UE de la Commission du 5 février 2010 ou tout document ultérieur publié par la Commission européenne. Les Clauses contractuelles types en vigueur à la date d'entrée en vigueur de l'Accord sont jointes en annexe aux CPD.

17.15. "**Sous-traitant ultérieur**" désigne tout autre sous-traitant engagé par Siemens et ayant accès à des Données à caractère personnel.

17.16. "**Catégories particulières de Données à caractère personnel**" désigne les informations qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les mesures de sécurité sociale, les procédures et sanctions administratives ou pénales, ou les données génétiques, les données biométriques aux fins d'identifier de manière unique une personne physique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

17.17. "**Garanties de transfert**" désigne (i) une décision d'adéquation au sens de l'article 45 du Règlement général sur la protection des données (UE) 2016/679 ou (ii) les garanties appropriées requises par l'article 46 du Règlement général sur la protection des données (UE) 2016/679.

17.18. "**Transferts vers des destinataires hors de l'EEE**" désigne (i) le Traitement de Données à caractère personnel en dehors de l'EEE ou d'un pays faisant l'objet d'une décision d'adéquation ou (ii) tout accès à des Données à caractère personnel en dehors de l'EEE ou d'un pays faisant l'objet d'une décision d'adéquation par Siemens ou l'un de ses Sous-traitants ultérieurs.

Annexes des CPD - Description des Opérations de Traitement

Cette Annexe précise l'objet du traitement, la nature et la finalité du traitement, le type de Données à caractère personnel et les catégories de personnes concernées. Les parties peuvent fournir d'autres détails dans l'Accord si cela est nécessaire pour une Offre particulière.

Objet, nature et finalité du traitement

Siemens et ses Sous-traitants ultérieurs traiteront les Données à caractère personnel pour fournir les Offres, y compris :

- les Offres accessibles par Internet ou des Offres similaires mises à disposition et hébergées par Siemens ("**Offres cloud**") ; ou
- les Offres d'administration, de gestion, d'installation, de configuration, de migration, de maintenance et de support ou toute autre Offre nécessitant un accès (à distance) aux Données à caractère personnel stockées dans les Offres cloud ou sur les systèmes informatiques du Client ("**Offres professionnelles et de support**").

Personnes concernées

Les Données à caractère personnel traitées concernent les catégories suivantes de Personnes concernées :

Les personnes concernées sont les suivantes :

- Les employés
- Les prestataires
- Les fournisseurs
- Les partenaires commerciaux
- Tout autre personne dont les Données à caractère personnel sont stockées sur les Offres et/ou sont traitées dans le cadre de la fourniture des Offres

Catégories de données

Les Données à caractère personnel traitées concernent les catégories suivantes de Données à caractère personnel :

- Les informations relatives aux contacts et aux utilisateurs, notamment le nom, le numéro de téléphone, l'adresse électronique, le fuseau horaire et les coordonnées postales
- L'accès au système, l'utilisation, les données d'autorisation, les données d'exploitation et tout fichier journal du système contenant des Données à caractère personnel ou toute autre donnée spécifique à l'application que les utilisateurs saisissent dans les Offres
- Le cas échéant, d'autres Données à caractère personnel telles que déterminées par le Client et ses autres Responsables du traitement en les téléchargeant ou en les connectant aux Offres ou en y donnant accès de toute autre manière via les Offres.

Catégories particulières de Données à caractère personnel (le cas échéant)

Les Offres ne sont pas destinées au traitement de Catégories particulières de Données à caractère personnel et le Client et ses autres Responsables du traitement ne doivent pas nous transférer, directement ou indirectement, de telles Données à caractère personnel sensibles.

Annexes des CPD - Liste des Sous-traitants ultérieurs approuvés

Une référence aux Sous-traitants ultérieurs que nous utilisons pour fournir l'Offre est disponible à l'adresse suivante www.siemens.com/DPT ou contenue dans l'Accord concerné.

Annexes des CPD - Mesures techniques et organisationnelles

Ce document décrit les mesures techniques et organisationnelles (MTO) mises en œuvre par Siemens et ses Sous-traitants ultérieurs pour protéger les systèmes et applications informatiques de Siemens et de ses Sous-traitants ultérieurs. Certaines Offres peuvent être protégées par des MOT différentes ou supplémentaires, telles que définies dans l'Accord correspondant.

Scénario 1 : MOT applicables aux Offres cloud.

Scénario 2 : MOT applicables aux Offres professionnelles et de support fournies via des outils d'accès à distance fournis et contrôlés par Siemens.

Scénario 3 : MOT applicables aux Offres professionnelles et de support fournies via des outils d'accès à distance fournis et contrôlés par le Client.

#	Mesures	Scénario		
		1	2	3
1. Sécurité physique et environnementale				
	Siemens met en œuvre des mesures appropriées pour empêcher les personnes non autorisées d'accéder aux équipements de traitement des données (à savoir les serveurs de bases de données et d'applications et le matériel connexe). Elle y veille en :			
	a) établissant des zones de sécurité ;	X	X	-
	b) protégeant et limitant les voies d'accès ;	X	X	-
	c) sécurisant les équipements informatiques et les ordinateurs décentralisés ;	X	X	X
	d) mettant en place des autorisations d'accès pour les employés et les tiers, y compris à la documentation correspondante ;	X	X	-
	e) tous les accès au centre de données où sont hébergées les Données à caractère personnel seront enregistrés, surveillés et suivis ;	X	-	-
	f) le centre de données où sont hébergées les Données à caractère personnel est sécurisé par des contrôles d'accès restreints et d'autres mesures de sécurité appropriées ;	X	-	-
	g) la maintenance et l'inspection des équipements de support dans les espaces informatiques et les centres de données ne peuvent être effectuées que par le personnel autorisé.	X	X	-
2. Contrôle d'accès (systèmes informatiques et/ou applications informatiques)				
	2.1 Siemens met en œuvre un système d'autorisation et d'authentification comprenant, sans s'y limiter, les éléments suivants :			
	a) la mise en place de contrôles d'accès basés sur les rôles ;	X	X	X
	b) la mise en place d'un processus de création, de modification et de suppression de comptes ;	X	X	X
	c) la protection, par des mécanismes d'authentification, de l'accès aux systèmes et applications informatiques ;	X	X	X
	d) l'utilisation de méthodes d'authentification adaptées aux caractéristiques et aux possibilités techniques du système ou de l'application informatique ;	X	X	X
	e) un accès aux systèmes et applications informatiques par authentification ;	X	X	X
	f) l'enregistrement de tout accès aux données (y compris les Données à caractère personnel) ;	X	X	-
	g) la mise en œuvre de mesures d'autorisation et de journalisation des connexions réseau entrantes et sortantes aux systèmes et applications informatiques (y compris des pare-feu permettant d'autoriser ou de refuser les connexions réseau entrantes) ;	X	X	-

#	Mesures	Scénario		
		1	2	3
	h) les droits d'accès privilégiés aux systèmes informatiques, aux applications et aux Offres de réseau ne sont accordés qu'aux personnes qui en ont besoin pour accomplir leurs tâches (principe du moindre privilège) ;	X	X	X
	i) les droits d'accès privilégiés aux systèmes et applications informatiques sont enregistrés et tenus à jour ;	X	X	X
	j) les droits d'accès aux systèmes et applications informatiques sont revus et mis à jour régulièrement ;	X	X	X
	k) la mise en œuvre d'une politique en matière de mots de passe, y compris des exigences relatives à la complexité des mots de passe, à leur longueur minimale et à leur expiration après une période adéquate, à la non-réutilisation de mots de passe récemment utilisés ;	X	X	X
	l) les systèmes et applications informatiques appliquent techniquement la politique de mot de passe ;	X	X	X
	m) politique de verrouillage du terminal de l'utilisateur lorsque ce dernier quitte le lieu de travail ;	X	X	X
	n) arrêt automatique du terminal de l'utilisateur s'il reste inactif ;	X	X	X
	o) désactivation automatique de l'identification de l'utilisateur lorsque plusieurs mots de passe erronés sont saisis, avec un fichier journal des événements (surveillance des tentatives d'intrusion) ;	X	X	X
	p) les droits d'accès des employés et du personnel externe aux systèmes et applications informatiques sont supprimés dès la fin de l'emploi ou du contrat ;	X	X	X
	q) utilisation de certificats d'authentification sécurisés de l'état de l'art.	X	X	-
	2.2 Siemens met en œuvre un concept de rôles et de responsabilités.	X	X	-
	2.3 Les systèmes et applications informatiques se verrouillent automatiquement ou mettent fin à la session après un délai d'inactivité raisonnable.	X	X	-
	2.4 Siemens suit des procédures de connexion sur les systèmes informatiques avec des garanties contre les activités de connexion suspectes (par exemple, contre les attaques par force brute et les attaques par mot de passe au hasard).	X	X	X
3. Contrôle de la disponibilité				
	3.1 Siemens définit, documente et met en œuvre un concept de sauvegarde pour les systèmes informatiques, comprenant les éléments techniques et organisationnels suivants :			
	a) Les supports de stockage des sauvegardes sont protégés contre les accès non autorisés et les menaces environnementales (par exemple, chaleur, humidité, incendie).	X	-	-
	b) Des intervalles de sauvegarde sont définis.	X	-	-
	c) La restauration des données à partir des sauvegardes est testée régulièrement en fonction de la criticité du système ou de l'application informatique.	X	-	-
	3.2 Siemens stocke les sauvegardes dans un lieu physique différent de celui où est hébergé le système de production.	X	-	-
	3.3 Siemens met en œuvre des solutions anti-malware de l'état de l'art pour protéger ses systèmes et applications contre les logiciels malveillants.	X	X	X
	3.4 Les systèmes et applications informatiques des environnements de non-production sont séparés logiquement ou physiquement des systèmes et applications informatiques des environnements de production.	X	-	-
	3.5 Les centres de données dans lesquels les Données à caractère personnel sont stockées ou traitées sont protégés contre les catastrophes naturelles, les attaques physiques ou les accidents.	X	-	-

#	Mesures	Scénario		
		1	2	3
	3.6 Les équipements de soutien dans les espaces informatiques et les centres de données, tels que les câbles, l'électricité, les installations de télécommunication, l'approvisionnement en eau ou les systèmes de climatisation, sont protégés contre les perturbations et les manipulations non autorisées.	X	-	-
4. Sécurité des opérations				
	4.1 Siemens maintient et met en œuvre un cadre de sécurité de l'information ISO 27001 à l'échelle de l'entreprise, qui est régulièrement révisé et mis à jour.	X	X	X
	4.2 Siemens enregistre les événements relatifs à la sécurité, tels que les activités de gestion des utilisateurs (par exemple, création, suppression), les échecs de connexion, les modifications de la configuration de sécurité du système sur les systèmes et applications informatiques.	X	X	X
	4.3 Siemens analyse en permanence les données des journaux des applications et des systèmes informatiques respectifs pour détecter les anomalies, les irrégularités, les indicateurs de compromission et les autres activités suspectes.	X	X	X
	4.4 Siemens scanne et teste régulièrement les systèmes et applications informatiques pour détecter les failles de sécurité.	X	X	X
	4.5 Siemens met en œuvre et maintient un processus de gestion des changements pour les systèmes et applications informatiques.	X	X	X
	4.6 Siemens maintient un processus de mise à jour et de mise en œuvre des correctifs de sécurité et des mises à jour des fournisseurs sur les systèmes et applications informatiques respectifs.	X	X	X
	4.7 Siemens efface irrémédiablement les données ou détruit physiquement les supports de stockage des données avant de mettre au rebut ou de réutiliser un système informatique.	X	X	X
5. Commandes de transmission				
	5.1 Siemens surveille en permanence et systématiquement les systèmes informatiques, les applications et les zones de réseau concernées afin de détecter toute activité malveillante ou anormale sur le réseau par :			
	a) pare-feu (par exemple, pare-feu à états, pare-feu d'application) ;	X	X	-
	b) serveurs proxy ;	X	X	-
	c) systèmes de détection des intrusions (IDS) et/ou systèmes de prévention des intrusions (IPS) ;	X	X	-
	d) filtrage des URL ;	X	-	-
	e) systèmes de gestion des informations et des événements de sécurité (SIEM).	X	X	-
	5.2 Siemens documente et met à jour régulièrement les topologies de réseau et ses exigences en matière de sécurité.	X	X	-
	5.3 Siemens administre les systèmes et applications informatiques en utilisant des connexions cryptées de l'état de l'art.	X	X	-
	5.4 Siemens protège l'intégrité du contenu pendant la transmission par des protocoles de réseau de l'état de l'art, tels que TLS.	X	X	-
	5.5 Siemens chiffre, ou permet à ses clients de chiffrer, les données des clients qui sont transmises sur des réseaux publics.	X	X	-
	5.6 Siemens utilise des systèmes de gestion des clés (Key Management Systems, KMS) sécurisés pour stocker les clés secrètes sur le cloud.	X	-	-
6. Incidents de sécurité				
	Siemens maintient et met en œuvre un processus de traitement des incidents, comprenant, entre autres :			

#	Mesures	Scénario		
		1	2	3
	a) les enregistrements des violations de la sécurité ;	X	X	X
	b) les processus de notification des clients ;	X	X	X
	c) un plan d'intervention en cas d'incident pour traiter les points suivants au moment de l'incident : (i) rôles, responsabilités et stratégies de communication et de contact en cas de compromission ; (ii) procédures spécifiques d'intervention en cas d'incident ; et (iii) couverture et réponses de tous les composants critiques du système.	X	X	X
7. Gestion des actifs, acquisition, développement et maintenance des systèmes				
	7.1 Siemens met en œuvre un processus de correction de sécurité adéquat qui comprend :			
	a) la surveillance des composants pour les faiblesses potentielles (CVE) ;	X	X	-
	b) le degré de priorité du correctif ;	X	X	-
	c) la mise en œuvre opportune du correctif ;	X	X	-
	d) le téléchargement de correctifs à partir de sources fiables.	X	X	-
	7.2 Siemens identifie et documente les exigences en matière de sécurité des informations avant le développement et l'acquisition de nouveaux systèmes et applications informatiques, ainsi qu'avant d'apporter des améliorations aux systèmes et applications informatiques existants.	X	X	-
	7.3 Siemens met en place un processus formel pour contrôler et effectuer les modifications des applications développées.	X	X	-
	7.4 Siemens planifie et intègre des tests de sécurité dans le cycle de vie du développement des systèmes et applications informatiques.	X	X	-
8. Sécurité des ressources humaines				
	8.1 Siemens met en œuvre les mesures suivantes dans le domaine de la sécurité des ressources humaines :			
	a) Les employés ayant accès aux Données à caractère personnel sont liés par des obligations de confidentialité.	X	X	X
	b) Les employés ayant accès aux Données à caractère personnel sont régulièrement formés aux lois et règlements applicables en matière de protection des données.	X	X	X
	8.2 Siemens met en œuvre un processus de désengagement pour ses employés et ses fournisseurs externes.	X	X	X

Annexes des CPD - Aperçu du RGPD

Le tableau suivant présente les articles pertinents du RGPD et les termes correspondants des CPD à des fins d'illustration.

#	Référence RGPD	Section des CPD	Titre
1.	Article 28 1)	Section 4 et Annexes des CPD	Mesures techniques et organisationnelles et Annexes des CPD
2.	Article 28 2), 3) d) et 4)	Section 6	Sous-traitants ultérieurs
3.	Article 28 3), première phrase	Section 2 et Annexes des CPD	Détails du traitement et Annexes des CPD
4.	Articles 28 3) a) et 29	Section 3	Instructions
5.	Article 28 3) b)	Section 5	Confidentialité du traitement
6.	Articles 28 3) c) et 32	Section 4 et Annexes des CPD relatives à la Sécurité	Mesures techniques et organisationnelles et Annexes des CPD
7.	Article 28 3) e)	Section 9.1	Droits des personnes concernées
8.	Articles 28 3) f) et 32	Section 9.2, Section 4 et Annexes des CPD	Assistance Siemens et Annexes des CPD
9.	Articles 28 3) f) et 33 à 34	Section 8	Violation des Données à caractère personnel
10.	Articles 28 3) f) et 35 à 36	Section 9.2	Assistance Siemens
11.	Article 28 3) g)	Section 14	Durée et résiliation
12.	Article 28 3) h)	Section 10	Audits
13.	Article 28 4)	Section 6	Sous-traitants ultérieurs
14.	Article 46 1) b) et c)	Section 7 et Annexes des CPD - Clauses contractuelles types	Transferts vers des bénéficiaires hors de l'EEE et Annexes des CPD - Clauses contractuelles types

Annexe – CLAUSES CONTRACTUELLES TYPES (SOUS-TRAITANTS)

Aux fins de l'article 26, paragraphe 2 de la directive 95/46/CE pour le transfert des données à caractère personnel vers des sous-traitants établis dans des pays tiers qui n'assurent pas un niveau adéquat de protection des données

Clause première Définitions

Au sens des clauses:

- (a) «données à caractère personnel», «catégories particulières de données», «traiter/traitement», «responsable du traitement», «sous-traitant», «personne concernée» et «autorité de contrôle» ont la même signification que dans la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données;
- (b) l'«exportateur de données» est le responsable du traitement qui transfère les données à caractère personnel;
- (c) l'«importateur de données» est le sous-traitant qui accepte de recevoir de l'exportateur de données des données à caractère personnel destinées à être traitées pour le compte de ce dernier après le transfert conformément à ses instructions et aux termes des présentes clauses et qui n'est pas soumis au mécanisme d'un pays tiers assurant une protection adéquate au sens de l'article 25, paragraphe 1, de la directive 95/46/CE;
- (d) le «sous-traitant ultérieur» est le sous-traitant engagé par l'importateur de données ou par tout autre sous-traitant ultérieur de celui-ci, qui accepte de recevoir de l'importateur de données ou de tout autre sous-traitant ultérieur de celui-ci des données à caractère personnel exclusivement destinées à des activités de traitement à effectuer pour le compte de l'exportateur de données après le transfert conformément aux instructions de ce dernier, aux conditions énoncées dans les présentes clauses et selon les termes du contrat de sous-traitance écrit;
- (e) le «droit applicable à la protection des données» est la législation protégeant les libertés et les droits fondamentaux des personnes, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans l'État membre où l'exportateur de données est établi;
- (f) les «mesures techniques et d'organisation liées à la sécurité» sont les mesures destinées à protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement.

Clause 2 Détails du transfert

Les détails du transfert et, notamment, le cas échéant, les catégories particulières de données à caractère personnel, sont spécifiés dans l'appendice 1 qui fait partie intégrante des présentes clauses.

Clause 3 Clause du tiers bénéficiaire

1. La personne concernée peut faire appliquer contre l'exportateur de données la présente clause, ainsi que la clause 4, points b) à i), la clause 5, points a) à e) et points g) à j), la clause 6, paragraphes 1 et 2, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12 en tant que tiers bénéficiaire.
2. La personne concernée peut faire appliquer contre l'importateur de données la présente clause, ainsi que la clause 5, points a) à e) et g), la clause 6, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12 dans les cas où l'exportateur de données a matériellement disparu ou a cessé d'exister en droit, à moins que l'ensemble de ses obligations juridiques n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, à laquelle reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre laquelle la personne concernée peut donc faire appliquer lesdites clauses.
3. La personne concernée peut faire appliquer contre le sous-traitant ultérieur la présente clause, ainsi que la clause 5, points a) à e) et g), la clause 6, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12, mais uniquement dans les cas où l'exportateur de données et l'importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, à moins que l'ensemble des obligations juridiques de l'exportateur de données n'ait été transféré, par contrat ou par effet de la loi, au successeur légal, auquel reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre lequel la personne concernée peut donc faire appliquer lesdites clauses. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.
4. Les parties ne s'opposent pas à ce que la personne concernée soit représentée par une association ou un autre organisme si elle en exprime le souhait et si le droit national l'autorise.

Clause 4 Obligations de l'exportateur de données

L'exportateur de données accepte et garantit ce qui suit:

- (a) le traitement, y compris le transfert proprement dit des données à caractère personnel, a été et continuera d'être effectué conformément aux dispositions pertinentes du droit applicable à la protection des données (et, le cas échéant, a été notifié aux autorités compétentes de l'État membre dans lequel l'exportateur de données est établi) et n'enfreint pas les dispositions pertinentes dudit État;
- (b) il a chargé, et chargera pendant toute la durée des services de traitement de données à caractère personnel, l'importateur de données de traiter les données à caractère personnel transférées pour le compte exclusif de l'exportateur de données et conformément au droit applicable à la protection des données et aux présentes clauses;
- (c) l'importateur de données offrira suffisamment de garanties en ce qui concerne les mesures techniques et d'organisation liées à la sécurité spécifiées dans l'appendice 2 du présent contrat;

- (d) après l'évaluation des exigences du droit applicable à la protection des données, les mesures de sécurité sont adéquates pour protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement et elles assurent un niveau de sécurité adapté aux risques liés au traitement et à la nature des données à protéger, eu égard au niveau technologique et au coût de mise en œuvre;
- (e) il veillera au respect des mesures de sécurité;
- (f) si le transfert porte sur des catégories particulières de données, la personne concernée a été informée ou sera informée avant le transfert ou dès que possible après le transfert que ses données pourraient être transmises à un pays tiers n'offrant pas un niveau de protection adéquat au sens de la directive 95/46/CE;
- (g) il transmettra toute notification reçue de l'importateur de données ou de tout sous-traitant ultérieur conformément à la clause 5, point b), et à la clause 8, paragraphe 3), à l'autorité de contrôle de la protection des données s'il décide de poursuivre le transfert ou de lever sa suspension;
- (h) il mettra à la disposition des personnes concernées, si elles le demandent, une copie des présentes clauses, à l'exception de l'appendice 2, et une description sommaire des mesures de sécurité, ainsi qu'une copie de tout contrat de sous-traitance ultérieure ayant été conclu conformément aux présentes clauses, à moins que les clauses ou le contrat ne contienne(nt) des informations commerciales, auquel cas il pourra retirer ces informations;
- (i) en cas de sous-traitance ultérieure, l'activité de traitement est effectuée conformément à la clause 11 par un sous-traitant ultérieur offrant au moins le même niveau de protection des données à caractère personnel et des droits de la personne concernée que l'importateur de données conformément aux présentes clauses; et
- (j) il veillera au respect de la clause 4, points a) à i).

Clause 5
Obligations de l'importateur de données

L'importateur de données accepte et garantit ce qui suit:

- (a) il traitera les données à caractère personnel pour le compte exclusif de l'exportateur de données et conformément aux instructions de ce dernier et aux présentes clauses; s'il est dans l'incapacité de s'y conformer pour quelque raison que ce soit, il accepte d'informer dans les meilleurs délais l'exportateur de données de son incapacité, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat;
- (b) il n'a aucune raison de croire que la législation le concernant l'empêche de remplir les instructions données par l'exportateur de données et les obligations qui lui incombent conformément au contrat, et si ladite législation fait l'objet d'une modification susceptible d'avoir des conséquences négatives importantes pour les garanties et les obligations offertes par les clauses, il communiquera la modification à l'exportateur de données sans retard après en avoir eu connaissance, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat
- (c) il a mis en œuvre les mesures techniques et d'organisation liées à la sécurité spécifiées dans l'appendice 2 avant de traiter les données à caractère personnel transférées;
- (d) il communiquera sans retard à l'exportateur de données:

- (i) toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre, sauf disposition contraire, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière;
 - (ii) tout accès fortuit ou non autorisé; et
 - (iii) toute demande reçue directement des personnes concernées sans répondre à cette demande, à moins qu'il n'ait été autorisé à le faire;
- (e) il traitera rapidement et comme il se doit toutes les demandes de renseignements émanant de l'exportateur de données relatives à son traitement des données à caractère personnel qui font l'objet du transfert et se rangera à l'avis de l'autorité de contrôle en ce qui concerne le traitement des données transférées;
 - (f) à la demande de l'exportateur de données, il soumettra ses moyens de traitement de données à une vérification des activités de traitement couvertes par les présentes clauses qui sera effectuée par l'exportateur de données ou un organe de contrôle composé de membres indépendants possédant les qualifications professionnelles requises, soumis à une obligation de secret et choisis par l'exportateur de données, le cas échéant, avec l'accord de l'autorité de contrôle;
 - (g) il mettra à la disposition de la personne concernée, si elle le demande, une copie des présentes clauses, ou tout contrat de sous-traitance ultérieure existant, à moins que les clauses ou le contrat ne contienne(nt) des informations commerciales, auquel cas il pourra retirer ces informations, à l'exception de l'appendice 2, qui sera remplacé par une description sommaire des mesures de sécurité, lorsque la personne concernée n'est pas en mesure d'obtenir une copie de l'exportateur de données;
 - (h) en cas de sous-traitance ultérieure, il veillera au préalable à informer l'exportateur de données et à obtenir l'accord écrit de ce dernier;
 - (i) les services de traitement fournis par le sous-traitant ultérieur seront conformes à la clause 11;
 - (j) il enverra dans les meilleurs délais une copie de tout accord de sous-traitance ultérieure conclu par lui en vertu des présentes clauses à l'exportateur de données.

Clause 6
Responsabilité

1. Les parties conviennent que toute personne concernée ayant subi un dommage du fait d'un manquement aux obligations visées à la clause 3 ou à la clause 11 par une des parties ou par un sous-traitant ultérieur a le droit d'obtenir de l'exportateur de données réparation du préjudice subi.
2. Si une personne concernée est empêchée d'intenter l'action en réparation visée au paragraphe 1 contre l'exportateur de données pour manquement par l'importateur de données ou par son sous-traitant ultérieur à l'une ou l'autre de ses obligations visées à la clause 3 ou à la clause 11, parce que l'exportateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'importateur de données accepte que la personne concernée puisse déposer une plainte à son encontre comme s'il était l'exportateur de données, à moins que l'ensemble des obligations juridiques de l'exportateur de données n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, contre laquelle la personne concernée peut alors faire valoir ses droits.

L'importateur de données ne peut invoquer un manquement par un sous-traitant ultérieur à ses obligations pour échapper à ses propres responsabilités.

3. Si une personne concernée est empêchée d'intenter l'action visée aux paragraphes 1 et 2 contre l'exportateur de données ou l'importateur de données pour manquement par le sous-traitant ultérieur à l'une ou l'autre de ses obligations visées à la clause 3 ou à la clause 11, parce que l'exportateur de données et l'importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, le sous-traitant ultérieur accepte que la personne concernée puisse déposer une plainte à son encontre en ce qui concerne ses propres activités de traitement conformément aux présentes clauses comme s'il était l'exportateur de données ou l'importateur de données, à moins que l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données n'ait été transféré, par contrat ou par effet de la loi, au successeur légal, contre lequel la personne concernée peut alors faire valoir ses droits. La responsabilité du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

Clause 7 **Médiation et juridiction**

1. L'importateur de données convient que si, en vertu des clauses, la personne concernée invoque à son encontre le droit du tiers bénéficiaire et/ou demande réparation du préjudice subi, il acceptera la décision de la personne concernée:
 - (a) de soumettre le litige à la médiation d'une personne indépendante ou, le cas échéant, de l'autorité de contrôle;
 - (b) de porter le litige devant les tribunaux de l'État membre où l'exportateur de données est établi.
2. Les parties conviennent que le choix effectué par la personne concernée ne remettra pas en cause le droit procédural ou matériel de cette dernière d'obtenir réparation conformément à d'autres dispositions du droit national ou international.

Clause 8 **Coopération avec les autorités de contrôle**

1. L'exportateur de données convient de déposer une copie du présent contrat auprès de l'autorité de contrôle si celle-ci l'exige ou si ce dépôt est prévu par le droit applicable à la protection des données.
2. Les parties conviennent que l'autorité de contrôle a le droit d'effectuer des vérifications chez l'importateur de données et chez tout sous-traitant ultérieur dans la même mesure et dans les mêmes conditions qu'en cas de vérifications opérées chez l'exportateur de données conformément au droit applicable à la protection des données.
3. L'importateur de données informe l'exportateur de données, dans les meilleurs délais, de l'existence d'une législation le concernant ou concernant tout sous-traitant ultérieur faisant obstacle à ce que des vérifications soient effectuées chez lui ou chez tout sous-traitant ultérieur conformément au paragraphe 2. Dans ce cas, l'exportateur de données a le droit de prendre les mesures prévues par la clause 5, point b).

Clause 9 **Droit applicable**

Les clauses sont régies par le droit de l'État membre où l'exportateur de données est établi.

Clause 10 **Modification du contrat**

Les parties s'engagent à ne pas modifier les présentes clauses. Les parties restent libres d'inclure d'autres clauses à caractère commercial qu'elles jugent nécessaires, à condition qu'elles ne contredisent pas les présentes clauses.

Clause 11 **Sous-traitance ultérieure**

1. L'importateur de données ne sous-traite aucune de ses activités de traitement effectuées pour le compte de l'exportateur de données conformément aux présentes clauses sans l'accord écrit préalable de l'exportateur de données. L'importateur de données ne sous-traite les obligations qui lui incombent conformément aux présentes clauses, avec l'accord de l'exportateur de données, qu'au moyen d'un accord écrit conclu avec le sous-traitant ultérieur, imposant à ce dernier les mêmes obligations que celles qui incombent à l'importateur de données conformément aux présentes clauses. En cas de manquement, par le sous-traitant ultérieur, aux obligations en matière de protection des données qui lui incombent conformément audit accord écrit, l'importateur de données reste pleinement responsable du respect de ces obligations envers l'exportateur de données.
2. Le contrat écrit préalable entre l'importateur de données et le sous-traitant ultérieur prévoit également une clause du tiers bénéficiaire telle qu'énoncée à la clause 3 pour les cas où la personne concernée est empêchée d'intenter l'action en réparation visée à la clause 6, paragraphe 1, contre l'exportateur de données ou l'importateur de données parce que ceux-ci ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, et que l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données n'a pas été transféré, par contrat ou par effet de la loi, à une autre entité leur ayant succédé. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.
3. Les dispositions relatives aux aspects de la sous-traitance ultérieure liés à la protection des données du contrat visé au paragraphe 1 sont régies par le droit de l'État membre où l'exportateur de données est établi.
4. L'exportateur de données tient une liste des accords de sous-traitance ultérieure conclus en vertu des présentes clauses et notifiés par l'importateur de données conformément à la clause 5, point j), qui sera mise à jour au moins une fois par an. Cette liste est mise à la disposition de l'autorité de contrôle de la protection des données de l'exportateur de données.

Clause 12 **Obligation après la résiliation des services de traitement des données à caractère personnel**

1. Les parties conviennent qu'au terme des services de traitement des données, l'importateur de données et le sous-traitant ultérieur restitueront à l'exportateur de données, et à la convenance de celui-ci, l'ensemble des données à caractère personnel transférées ainsi que les copies, ou détruiront l'ensemble de ces données et en apporteront la preuve à l'exportateur de données, à moins que la législation imposée à l'importateur de données ne l'empêche de restituer ou de détruire la totalité ou une partie des données à caractère personnel transférées. Dans ce cas, l'importateur de données garantit qu'il assurera la confidentialité des données à caractère personnel transférées et qu'il ne traitera plus activement ces données.
2. L'importateur de données et le sous-traitant ultérieur garantissent que si l'exportateur de données et/ou l'autorité de contrôle le demandent, ils soumettront leurs moyens de traitement de données à une vérification des mesures visées au paragraphe 1.