ACCORD DE TRAITEMENT DES DONNÉES

Le présent Accord de traitement des données (ci-après dénommé « Accord ») est convenu entre Siemens Product Lifecycle Management Software Inc., aussi appelé Siemens Industry Software (ci-après dénommé « SISW »), et le Client (ci-après dénommé « Client ») qui a accepté les conditions du présent Accord. SISW se réserve le droit d'utiliser ses sociétés affiliées pour l'application de l'ensemble de ses droits et de ses obligations dans le cadre du présent Accord. Ainsi, le terme « SISW » utilisé dans le présent Accord peut également désigner les sociétés affiliées détenues ou contrôlées directement ou non par la société mère Siemens Product Lifecycle Management Software Inc. et qui ont été autorisées par Siemens Product Lifecycle Management Software Inc. à distribuer les services cloud de SISW (ci-après « service cloud »).

Il incombe uniquement au Client de déterminer le type de données et les personnes affectées par le traitement. En outre, le Client doit s'assurer de la légitimité d'un tel traitement par le biais du service cloud. Le Client est également responsable de toute correction, suppression ou blocage des données à caractère personnel lors de l'utilisation des fonctionnalités fournies par le service cloud. Le Client peut exporter et supprimer ses données, dont ses données à caractère personnel, à l'aide des fonctionnalités fournies par le service cloud. À l'expiration du présent Accord de traitement des données, le Client disposera de 30 jours pour envoyer une demande écrite à SISW afin que les données du Client puissent être téléchargées par ce dernier. Après expiration de la période définie par SISW en réponse à cette demande, toute donnée subsistante du Client pourra être supprimée et ne pourra plus être téléchargée par le Client. SISW et le Client acceptent que, dans le cadre du service cloud, le droit du Client à émettre des instructions soit exclusivement exercé par le biais des fonctionnalités fournies par le service cloud. Toute autre instruction concernant les données du Client nécessitera un accord écrit distinct entre SISW et le Client, dont un accord sur tout frais supplémentaire dû par le Client en cas d'émission d'une telle instruction. Le Client accepte de ne charger ni de stocker aucune donnée de santé protégée sur le service cloud, sauf accord écrit contraire entre SISW et le Client qui autoriserait expressément le stockage de données de santé protégées au sein du service cloud.

Lors de la fourniture du service cloud, en ce qui concerne le système de production, SISW se conformera aux mesures techniques et d'organisation décrites à l'appendice 2 de l'annexe A du présent Accord de traitement des données. Les systèmes non dédiés à la production associés au service cloud peuvent ne pas se conformer aux mesures décrites à l'appendice 2 de l'annexe A. De plus, SISW se réserve le droit de modifier régulièrement les mesures techniques et d'organisation applicables au système de production, à condition que de telles modifications n'affectent pas défavorablement et matériellement le niveau de protection de ces mesures. SISW n'autorisera son personnel à collecter, traiter et utiliser les données à caractère personnel sans permission et emploiera uniquement pour le traitement des données à caractère personnel du Client des personnes spécifiquement formées aux exigences de protection de la confidentialité des données.

SISW est habilité à engager des sous-traitants pour l'exécution du service cloud. Dans la mesure où l'accès des sous-traitants aux données à caractère personnel du Client ne peut être exclu, SISW fournira à la demande du Client une liste de ses sous-traitants et de leurs sites respectifs, et mettra à jour cette liste dès que nécessaire avant que tout nouveau sous-traitant ne soit autorisé à accéder aux données à caractère personnel du Client. Dans l'éventualité où le Client s'opposerait raisonnablement à tout nouveau sous-traitant, le Client devra informer SISW de son opposition et, dans le cas où SISW persisterait à engager le nouveau sous-traitant, le Client aura le droit de résilier le présent Accord de traitement des données pour raison valable. Dans le cas où l'engagement d'un tel sous-traitant impliquerait le transfert de données à caractère personnel à l'étranger, SISW s'efforcera d'exiger du sous-traitant qu'il maintienne un niveau de protection des données adéquat au regard de ces données à caractère personnel.

SISW vérifiera régulièrement le respect des mesures techniques et d'organisation applicables et confirmera, à la demande raisonnable du Client, que ces mesures sont respectées. Dans le cas où le Client aurait raison de penser qu'une confirmation émise par SISW serait inexacte, le Client aura le droit de confirmer le respect des mesures techniques et d'organisation en planifiant un audit auprès de SISW, soumis à un préavis raisonnable. Un tel audit devra être exécuté aux frais du Client.

SISW et le Client acceptent que tout transfert des données à caractère personnel du Client d'un pays de l'Union Européenne vers un pays tiers, et dont l'UE considère le niveau de protection des données inadéquat, sera exécuté selon les conditions des clauses contractuelles types de l'UE, définies dans l'Annexe A et entièrement intégrées aux présentes. Dans l'éventualité d'un conflit entre les conditions du présent Accord de traitement des données et les clauses contractuelles types, les termes des clauses contractuelles types prévaudront. Les clauses contractuelles types seront régies par les lois de l'État membre de l'UE dans lequel l'exportateur des données (tel que défini dans l'Annexe A) est établi.

Annexe A
Clauses contractuelles types de l'UE

Aux fins de l'article 26(2) de la directive 95/46/EC relative au transfert des données à caractère personnel vers des sous-traitants établis dans des pays tiers qui n'assurent pas un niveau de protection des données adéquat

par et entre

le Client et/ou une société affiliée du Client basé dans l'UE

(ci-après dénommé « **l'exportateur de données** »)

et

Siemens Product Lifecycle Management Software Inc., aussi dénommé Siemens Industry Software, y compris toute société affiliée détenue ou contrôlée directement ou indirectement par la société mère Siemens Product Lifecycle Management Software Inc. et qui a été autorisée par Siemens Product Lifecycle Management Software Inc. à traiter les données pour son compte

(ci-après dénommé « **l'importateur de données** »),

ci-après dénommés individuellement une « partie » et collectivement les « parties »

SONT CONVENUS des clauses contractuelles suivantes (ci-après dénommées « les clauses ») afin d'offrir des garanties adéquates concernant la protection de la vie privée et des libertés et droits fondamentaux des personnes lors du transfert, par l'exportateur de données vers l'importateur de données, des données à caractère personnel visées à l'appendice 1.

Section 1. 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.

Section 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.

Section 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.

Section 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 Accord ;

(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).

Section 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.

Section 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.

Section 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.

Section 8. Coopération avec les autorités de contrôle

1. L'exportateur de données convient de déposer une copie du présent Accord 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).

Section 9. Droit applicable

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

Section 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.

Section 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.

Section 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.

APPENDICE 1 AUX CLAUSES CONTRACTUELLES TYPES

Exportateur de données
L'exportateur de données est (veuillez préciser brièvement vos activités qui présentent un intérêt pour le transfert) :

Le Client a souscrit un service cloud fourni par SISW, qui permet aux utilisateurs autorisés par le Client d'entrer, de modifier, d'utiliser, de supprimer, de télécharger ou de traiter les données du Client, pouvant inclure des données à caractère personnel, telles que définies dans le présent Accord et les documents relatifs au service cloud.

Importateur de données
L'importateur de données est (veuillez préciser brièvement vos activités qui présentent un intérêt pour le transfert) :

La société Siemens Product Lifecycle Management Software Inc. et/ou ses sous-traitants, fournissent le service cloud, incluant les prestations suivantes : maintenance de l'infrastructure informatique aux États-Unis et dans les pays de l'Union Européenne où le service cloud est opérationnel ; stockage au sein de l'infrastructure des données du Client chargées par ce dernier via le service cloud ; surveillance de la disponibilité et du fonctionnement continu du service cloud et de l'infrastructure ; et maintenance de l'infrastructure telle que définie dans le présent Accord et les documents relatifs au service cloud.

Personnes concernées
Les données à caractère personnel transférées concernent les catégories suivantes de personnes concernées (veuillez préciser) :

Sauf spécification contraire écrite par l'exportateur de données, les personnes concernées incluent les utilisateurs autorisés par le Client à utiliser les services cloud ainsi que les employés du Client dont les données à caractère personnel sont stockées sur le service cloud.

Catégories de données
Les données à caractère personnel transférées concernent les catégories suivantes de données (veuillez préciser) :

Les catégories de données spécifiques à stocker dans le service cloud sont sujettes à une configuration de grande envergure par le Client, bien que certaines catégories courantes de données susceptibles d'être stockées dans le service cloud puissent être, par exemple, les suivantes : nom, adresse électronique, nom de société, numéro de téléphone, lieu de travail, nationalité ou citoyenneté et informations relatives à l'accès et à l'utilisation du service cloud. En fonction de la configuration du service cloud du Client, de nombreuses autres catégories de données pourraient faire partie des données du Client.

Catégories spéciales de données (le cas échéant)
Les données à caractère personnel transférées concernent les catégories spéciales suivantes de données (veuillez préciser) :

Toute catégorie spéciale de données à stocker dans le service cloud serait comme convenu par les parties dans l'Accord ou dans une commande, ou tel qu'établi dans un énoncé de travail pour des services professionnels à fournir au Client dans le cadre du déploiement du service cloud.

Opérations de traitement
Les données à caractère personnel transférées seront sujettes aux activités de traitement de base suivantes (veuillez préciser) :

Les données à caractère personnel peuvent être : traitées dans le cadre du fonctionnement normal du service cloud, en fonction de la configuration du Client ; traitées par le biais du stockage et/ou de l'archivage sur l'infrastructure informatique maintenue par l'exportateur de données, dans des environnements pour client unique ou mutualisés ; consultées ou transmises en fonction des instructions émises pour le service cloud par un utilisateur que le Client autorise à utiliser le service cloud ; et traitées dans le cadre des opérations de maintenance du service cloud effectuées par l'exportateur de données.

APPENDICE 2 AUX CLAUSES CONTRACTUELLES TYPES

Certaines offres de services cloud sont fournies selon différentes conditions, lesquelles, si elles sont applicables, seront énoncées dans une commande. Dans le cas contraire, l'exportateur de données prendra les mesures techniques et organisationnelles décrites ci-dessous concernant les données à caractère personnel stockées dans le Système, conformément à la clause 4(d) et à la clause 5(c).

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par l'importateur de données conformément aux clauses 4(d) et 5(c) :

1. Contrôle de l'accès physique. Tout individu non autorisé se verra interdire l'accès physique aux locaux, bâtiments ou salles où se situent des systèmes de traitement des données qui traitent et/ou utilisent les données à caractère personnel.

   Mesures : Tous les centres de données respectent des procédures de sécurité strictes dont la mise en œuvre est assurée par du personnel de sécurité, des équipements de surveillance, des détecteurs de mouvement, des mécanismes de contrôle d'accès et d'autres mesures visant à empêcher que les installations des centres de données et les équipements soient compromis. Seuls des représentants autorisés peuvent accéder aux systèmes et à l'infrastructure au sein des installations des centres de données. Pour garantir un fonctionnement adéquat, des équipements de sécurité physique (par exemple, des détecteurs de mouvement et des caméras) sont régulièrement entretenus. De manière plus détaillée, les mesures de sécurité physique suivantes sont mises en œuvre sur l'ensemble des centres de données :

   a. En général, les bâtiments sont sécurisés par des systèmes de contrôle d'accès (système d'accès par carte à puce).
   b. Des preuves d'autorisation, parmi lesquelles peuvent figurer un badge d'accès électronique (unique à l'employé, au fournisseur ou au sous-traitant) et un code PIN, sont fournies au personnel autorisé pour accéder physiquement aux installations des centres de données.
   c. Tout accès physique aux centres de données à l'intérieur des frontières du système est régi par un système de contrôle d'accès électronique, qui comprend des lecteurs de cartes et des pavés de saisie de code PIN pour l'entrée dans les bâtiments et salles et de lecteurs de carte seulement pour la sortie des bâtiments et salles.
   d. En fonction de la classification de sécurité, les bâtiments, zones individuelles et lieux environnants sont également protégés par des mesures supplémentaires. Parmi ces mesures figurent des profils d'accès spécifiques, une vidéosurveillance, des systèmes d'alarme anti-intrusion et des systèmes de contrôle d'accès biométriques.
   e. Des droits d'accès seront octroyés au personnel autorisé individuellement, en fonction des mesures de contrôle d'accès aux systèmes et aux données énoncées ci-dessous. Cela s'applique aussi à l'accès des visiteurs. Les invités et visiteurs des bâtiments de SISW doivent inscrire leurs noms à la réception et être accompagnés par du personnel autorisé de SISW. La société SISW et tous les fournisseurs de centres de données tiers consignent les noms et heures d'entrée des personnes qui pénètrent dans les zones privées de SISW au sein des centres de données.
   f. Les employés et le personnel externe de SISW doivent se munir de leur carte d'identité sur tous les sites de SISW.

2. Contrôle de l'accès aux systèmes. Les systèmes de traitement des données utilisés pour fournir le service cloud ne doivent pas être utilisés sans autorisation.

   Mesures :
   a. SISW ou ses sous-traitants gère(nt) l'environnement de manière à se conformer aux exigences de contrôle d'accès,d'identification et d'authentification du NIST SP 800-53 Rev 4.
   b. Différents niveaux d'autorisation sont utilisés pour octroyer l'accès à des systèmes sensibles dont ceux stockant et traitant les données à caractère personnel. Des processus sont en place pour garantir que seuls des utilisateurs autorisés disposent de l'autorisation appropriée pour ajouter, supprimer ou modifier des utilisateurs.
   c. Tous les utilisateurs accèdent aux systèmes de SISW à l'aide d'un nom d'utilisateur unique et d'un mot de passe qui doit répondre à des critères de complexité minimum.
   d. SISW et ses sous-traitants disposent de procédures permettant de garantir que toute modification d'autorisation demandée soit mise en œuvre uniquement si elle respecte les lignes directrices (par exemple, aucun droit n'est octroyé sans autorisation). Si un utilisateur de SISW modifie des rôles ou quitte la société, un processus est mis en œuvre pour révoquer les droits d'accès à l'environnement.
   e. SISW et ses sous-traitants ont établi une stratégie de mot de passe qui empêche le partage de mots de passe, régit la procédure à suivre en cas de divulgation d'un mot de passe, exige des changements réguliers de tous les mots de passe des utilisateurs et requiert le changement des mots de passe par défaut. Des ID d'utilisateur

personnalisés sont attribués à des fins d'authentification. Tous les mots de passe doivent respecter des exigences de complexité minimum et être stockés sous une forme chiffrée. En cas de mots de passe de domaines, le système impose un changement de mot de passe tous les 60 jours dans le respect des exigences de complexité minimum. Chaque ordinateur de SISW dispose d'un économiseur d'écran protégé par un mot de passe.

f. La société SISW ou ses sous-traitants contrôle(nt) automatiquement les événements de compte suivants : création, modification, activation, désactivation et suppression. Un administrateur système examine régulièrement les journaux.
g. Les réseaux de SISW et de ses sous-traitants sont protégés de l'Internet public par des pare-feux.
h. SISW et ses sous-traitants utilisent des logiciels antivirus à jour au niveau des points d'accès au réseau.d'entreprise, pour les comptes de messagerie électronique et sur l'ensemble des serveurs de fichiers et des postes de travail.
i. SISW et ses sous-traitants appliquent une gestion de correctifs de sécurité pour veiller au déploiement des mises à jour de sécurité pertinentes.
j. L'accès à distance complet au réseau d'entreprise et à l'infrastructure critique de SISW est protégé par une authentification renforcée à facteurs multiples.

3. Contrôle de l'accès aux données. Le personnel autorisé à utiliser des systèmes de traitement des données n'aura accès qu'aux données à caractère personnel pour lesquelles il dispose d'un droit d'accès, et les données à caractère personnel ne devront pas être lues, copies, modifiées ou supprimées sans autorisation lors de leur traitement, de leur utilisation et de leur stockage.

   Mesures :

   a. L'accès aux informations personnelles, confidentielles ou sensibles est octroyé aux seules personnes qui en ont besoin. En d'autres termes, les employés ou tierces parties ont accès aux informations dont ils/elles ont besoin pour mener à bien leurs tâches. SISW utilise des concepts d'autorisation qui documentent la procédure d'attribution des autorisations et les autorisations attribuées. Toutes les données à caractère personnel, confidentielle ou sensible de quelque autre manière que ce soit sont protégées conformément aux stratégies et normes de sécurité de SISW.
   b. Tous les serveurs de production de tout service cloud de SISW sont exploités dans les centres de données pertinents. Les mesures de sécurité qui protègent les applications qui traitent des informations personnelles, confidentielles ou sensibles de quelque autre manière que ce soit sont régulièrement contrôlées. À cette fin, SISW incorpore également des audits externes réguliers pour confirmer que ces mesures sont correctement appliquées.
   c. SISW ne permet pas l'installation de logiciels personnels ou d'autres logiciels non approuvés par SISW sur des systèmes utilisés pour des services cloud.
   d. En cas de nécessité de transfert de données en raison d'une défaillance d'un support de stockage de données sous-jacent, une fois le transfert mené à bien, le support de stockage défectueux sera soit démagnétisé (dans le cas d'un stockage magnétique), soit déchiqueté (dans le cas d'un stockage SSD ou optique).

4. Contrôle de la transmission des données. Les données à caractère personnel ne doivent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant un transfert.

   Mesures :

   a. La société SISW ou son sous-traitant gèrera l'infrastructure et la configuration de manière à respecter les exigences de protection des systèmes et des communications du NIST SP 800-53 Rev 4. Cela comprend les systèmes de prévention des intrusions au niveau des réseaux (NIPS) et les pare-feux aux frontières des systèmes, lesquels assurent une protection contre les communications malveillantes à la frontière externe de l'infrastructure. Les NIPS et pare-feux sont configurés en fonction de normes STIG de l'agence DISA. Les données sont chiffrées en transit à l'aide de modules de chiffrement conformes à la norme FIPS 140-2.
   b. Lorsque des supports de données sont physiquement transportés, des mesures appropriées sont mises en œuvre chez SISW pour veiller au respect des niveaux de service convenus (par exemple, chiffrement ou contenants à revêtement de plomb).
   c. Les données à caractère personnel transmises sur des réseaux internes de SISW sont protégées de la même manière que n'importe quelle autre donnée confidentielle, conformément aux stratégies de sécurité de SISW.
   d. Quand les données sont transférées entre SISW et le Client, les mesures de protection dédiées aux données à caractère personnel transférées sont énoncées dans le contrat ou la documentation pertinente du service cloud concerné. Cela s'applique à la fois au transfert de données au niveau des réseaux et au transfert de données

physique. Le Client assume la responsabilité de tout transfert de données depuis le point de démarcation de SISW (par ex., le pare-feu sortant du centre de données qui héberge le service cloud).

5. Contrôle de l'entrée des données. Le service cloud permettra de déterminer rétrospectivement si et par qui des données à caractère personnel ont été entrées, modifiées ou supprimées au niveau de l'infrastructure utilisée pour fournir le service cloud.

   Mesures :
   a. Seule la société SISW permet au personnel autorisé d'accéder aux données à caractère personnel tel que l'exige le travail du personnel. SISW a mis en œuvre un système de journalisation pour l'entrée, la modification, la suppression ou le blocage des données à caractère personnel par SISW ou ses sous-traitants dans toute la mesure prise en charge par le service cloud.
   b. Des pistes d'audit fournissent le degré de détail requis pour faciliter la reconstruction d'événements en cas de survenue ou de soupçon d'activité non autorisée ou de dysfonctionnement. Chaque enregistrement de journal d'événements de système d'exploitation inclut le type d'événement, un horodatage, la source de l'événement, l'emplacement de l'événement, le résultat de l'événement et l'utilisateur associé à l'événement.

6. Contrôle des tâches. Les données à caractère personnel seront traitées uniquement en conformité avec les conditions des présentes et toute instruction associée fournie par le Client.

   Mesures :
   a. SISW exploite des contrôles et processus pour veiller au respect des contrats conclus entre SISW et ses clients, sous-traitants ou autres prestataires de service.
   b. Les données du Client seront soumises au moins au même niveau de protection que des informations confidentielles, conformément à la norme relative à la classification des informations de SISW.
   c. Tous les employés et partenaires contractuels de SISW sont contractuellement tenus de respecter la confidentialité de l'intégralité des informations sensibles, y compris des secrets commerciaux des clients et partenaires de SISW.

7. Contrôle de la disponibilité. Les données à caractère personnel seront protégées contre toute destruction ou perte accidentelle ou non autorisée.

   Mesures :
   a. SISW recourt à des processus de sauvegarde et à d'autres mesures qui garantissent la restauration rapide des systèmes essentiels à l'activité lorsque cela s'avère nécessaire.
   b. SISW se repose sur des prestataires de service cloud internationaux pour veiller à la disponibilité de l'alimentation des centres de données.
   c. SISW dispose de plans d'urgence définis, ainsi que de stratégies d'entreprise et de reprise après sinistre pour les services cloud.

8. Contrôle de la séparation des données. Les données à caractère personnel collectées à différentes fins peuvent être traitées séparément.

   Mesures :
   a. Lorsque cela est applicable, SISW recourt aux fonctionnalités techniques des logiciels déployés (par exemple, des environnements de systèmes mutualisés ou distincts) pour réaliser la séparation des données entre les données à caractère personnel du Client et celles de tout autre client.
   b. SISW maintient des instances dédiées (avec séparation logique ou physique) pour chaque client.
   c. Le Client (y compris ses sociétés affiliées) n'a accès qu'à sa/ses propre(s) instance(s) de client.

9. Contrôle de l'intégrité des données. Les données à caractère personnel resteront intactes, complètes et actuelles durant les activités de traitement.

   Mesures : SISW a mis en œuvre une stratégie de défense à plusieurs couches pour protéger contre les autorisations non autorisées. Cela renvoie aux contrôles tels qu'énoncés dans les sections relatives aux contrôles et mesures susmentionnées. De la configuration des pare-feux découleront plusieurs segments de réseau qui sépareront accès public et accès privé. Chaque ensemble de règles de pare-feu disposera de contrôles d'accès spécifiques, avec indication des communications autorisées entre ces segments.

a. Centre de contrôle de la sécurité : des logiciels de détection des intrusions automatisés seront utilisés conjointement à d'autres logiciels et processus criminalistiques et de prévention, afin d'alerter, d'enquêter et, le cas échéant, de notifier et d'aider à remédier à tout incident de sécurité.
b. Logiciels antivirus : tous les systèmes disposeront de définitions d'antivirus actuelles configurées pour assurer une protection contre les virus, les vers, les chevaux de Troie et d'autres formes de programmes malveillants.
c. Sauvegarde et récupération : tous les systèmes disposeront d'un niveau élémentaire d'instantanés de sauvegarde de données et de configuration. Le cas échéant, SISW et ses sous-traitants exploiteront aussi une instance de client avec une configuration à haute disponibilité qui garantira le stockage des données dans deux centres de données distincts à distance suffisante l'un de l'autre.
d. Audits externes réguliers des mesures de sécurité : SISW et ses sous-traitants réaliseront des audits externes réguliers pour tester les mesures de sécurité susmentionnées.