ACCORD DE TRAITEMENT DES DONNÉES

Sommaire

Accord de traitement des Données (« DPA »)

Entre_____ci-après dénommé le « **Responsable de Traitement** » et **SMART Technologies ULC**, ci-après dénommée le « **Sous-Traitant** ».

1. Contexte et objectif

1.1. Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« **RGPD** »), un accord écrit entre le Responsable de Traitement et le Sous-Traitant est nécessaire pour régir le traitement des données à caractère personnel que le Sous-Traitant effectue pour le compte du Responsable de Traitement.

1.2. Le présent DPA entre le Responsable de Traitement et le Sous-Traitant (« **les Parties** ») régit les obligations initiales du Sous-Traitant lorsqu'il traite des données à caractère personnel pour le compte du Responsable de Traitement. Le présent accord vise à garantir que le Sous-Traitant traite les données à caractère personnel conformément aux instructions du Responsable de Traitement et à la législation applicable, y compris la législation en vigueur au sein de l'UE/EEE, les différents règlements et décisions des autorités publiques et les recommandations du Comité européen de la protection des données (EDPB), qui s'appliquent au traitement des données à caractère personnel relevant du champ d'application du DPA.

1.3. Le Responsable de Traitement ne doit pas fournir de données sur les élèves au Sous-Traitant.

2. Définitions

2.1. Les définitions du présent DPA ont les définitions correspondantes telles qu'elles figurent dans le Le règlement général sur la protection des données (RGPD) est applicable et est mentionné ici.

3. Traitement des données à caractère personnel

3.1. Les Parties ont conclu le présent DPA afin de régir les conditions de traitement des données à caractère personnel par le Sous-Traitant conformément aux conditions de service et de confidentialité du Sous-Traitant applicable (« **TOSP** »), qui doivent être appliquées par le Sous-Traitant pour le compte du Responsable de Traitement.

3.2. Le Sous-Traitant et les personnes agissant pour le compte du Sous-Traitant, ne peuvent traiter les données à caractère personnel que conformément au DPA et à toutes les instructions écrites supplémentaires que le Responsable de Traitement peut donner de temps à autre.

3.3. Le Sous-Traitant ne traite les données à caractère personnel que pour s'acquitter de ses obligations conformément au TOSP. Si le Sous-Traitant n'a pas reçu d'instructions ou n'est pas sûr de la finalité du traitement nécessaire à l'exécution d'une certaine tâche qui implique ou pourrait impliquer le traitement de données à caractère personnel, il en informe sans délai le Responsable de Traitement et doit attendre que des instructions supplémentaires soient fournies par le Responsable de Traitement.

3.4. Le Sous-Traitant doit à tout moment respecter ses obligations en vertu de la législation applicable et se tenir informé de ces obligations en ce qui concerne le traitement des données à caractère personnel conformément au DPA. Le Sous-Traitant doit également se conformer à tout moment aux codes de conduite ou aux certifications qu'il s'est engagé à respecter. Le Sous-Traitant désigne, au moins dans le cadre du présent DPA, une personne de contact appropriée pour les questions spécifiques relatives à la protection des données.

3.5. Le Sous-Traitant s'engage à respecter le droit applicable, qui doit être interprété dans tous les cas en fonction de la nature des services fournis par le Sous-Traitant et qui implique généralement que le Sous-Traitant ne peut pas, à sa seule discrétion, collecter des données à caractère personnel ou utiliser des données à caractère personnel à des fins autres que l'exécution de la fourniture convenue conformément au contrat de revendeur principal (*reseller agreement*). En aucun cas, le Sous-Traitant ne peut, sans ordre d'une autorité compétente ou en l'absence d'un droit impératif

a) collecter ou transmettre des données à caractère personnel de ou à des tiers, sauf accord contraire écrit entre les Parties,

b) modifier la méthode de traitement des données à caractère personnel qui augmenterait le risque pour les libertés et droits fondamentaux des personnes concernées,

c) copier ou recréer des données à caractère personnel pour l'usage exclusif du Sous-Traitant ; ou

d) traiter de quelque manière que ce soit des données à caractère personnel à des fins autres que celles mentionnées dans les TOSP principales et les annexes y afférentes.

3.6. Le Sous-Traitant doit prendre toutes les mesures appropriées requises par l'article 32 du RGPD. Les mesures supplémentaires à prendre en compte sont indiquées dans les instructions en annexe du Responsable de Traitement.

3.7. Le Sous-Traitant assiste le Responsable de Traitement en mettant en œuvre, dans la mesure du possible, des mesures de sécurité techniques et organisationnelles appropriées pour permettre au Responsable de Traitement de remplir ses obligations en tant que Responsable de Traitement et ses obligations liées aux demandes d'exercice des droits des personnes concernées conformément au chapitre III du RGPD.

3.8. Le Sous-Traitant aide le Responsable de Traitement à veiller à ce que les obligations visées aux articles 33 à 36 du RGPD puissent être remplies, en tenant compte de la nature du traitement et des informations auxquelles le Sous-Traitant a accès.

4. Registre des activités de traitement

4.1. Le Sous-Traitant ou son représentant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de Traitement. Ce registre doit contenir au moins les informations suivantes :

a) le nom et les coordonnées du Sous-Traitant ou de tout Sous-Traitant ultérieur désigné, du Responsable de Traitement et du représentant du Responsable de Traitement ou du Sous-Traitant et du délégué à la protection des données ;

b) les catégories de traitements effectués pour le compte du Responsable de Traitement ;

c) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires situés dans des pays tiers ou, le cas échéant, des organisations internationales ;

d) la documentation des mesures appropriées prises lorsque des données à caractère personnel sont transférées vers un pays tiers qui ne figure pas dans une décision contenant des dispositions applicables relatives à un niveau de sécurité adéquat ou à des mesures de sécurité appropriées, et

e) le cas échéant, une description générale des mesures de sécurité techniques et organisationnelles prises par le Sous-Traitant conformément au droit applicable.

4.2. Le Sous-Traitant met ces registres à la disposition du Responsable de Traitement ou de l'autorité de contrôle compétente sur demande, en fournissant les informations susmentionnées.

4.3. Lorsqu'une personne concernée demande, dans l'exercice de ses droits, un inventaire du traitement de ses données à caractère personnel, le Sous-Traitant, après avoir consulté le Responsable de Traitement, met à disposition, à la demande de la personne concernée ou du Responsable de Traitement, un tel inventaire dont le contenu et les modalités sont conformes à la législation applicable.

5. Confidentialité et mesures de sécurité

5.1. Le Sous-Traitant met en œuvre les garanties techniques et organisationnelles nécessaires conformément au droit applicable et prend ainsi les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction, la perte ou l'altération accidentelles ou illicites, la divulgation non autorisée ou l'accès non autorisé aux données à caractère personnel transmises, stockées ou traitées d'une autre manière, notamment lorsque le traitement implique une adaptation ou une transmission de données via des réseaux et/ou un autre traitement illicite.

L'évaluation du niveau de sécurité approprié doit tenir compte des risques découlant du traitement, notamment la destruction, la perte ou l'altération accidentelles ou illicites, ainsi que la divulgation non autorisée de données à caractère personnel.

5.2. Le Sous-Traitant s'engage à traiter les données à caractère personnel de manière strictement confidentielle et à ne pas les transmettre ou les rendre accessibles à des tiers, à moins qu'une autorisation préalable n'ait été accordée ou que cela ne soit nécessaire d'une autre manière en vertu du droit applicable ou pour l'exécution du présent DPA.

5.3. Le Sous-Traitant s'engage à veiller à ce que seul le personnel concerné ait accès aux données à caractère personnel du Responsable de Traitement afin de remplir les obligations du Sous-Traitant en vertu du présent DPA. Le Sous-Traitant veille à ce que les employés autorisés à traiter les données à caractère personnel couvertes par le présent DPA soient tenus à la confidentialité, soit par la loi, soit par un accord correspondant aux règles de confidentialité énoncées dans le présent DPA. Le Sous-Traitant veille également à ce que son personnel comprenne l'importance de la confidentialité définie dans le présent accord de confidentialité. La confidentialité que les Parties s'engagent à respecter dans le DPA s'applique également à une période postérieure à l'expiration du présent DPA. Elle ne s'applique toutefois que pour une période définie par la législation en vigueur.

5.4. Le Sous-Traitant ne peut transférer des données à caractère personnel en dehors de l'UE / de l'EEE ou vers un pays qui ne figure pas sur la liste des pays exemptés d'un tel transfert en vertu de la législation applicable, sans (i) le consentement écrit préalable du Responsable de Traitement et (ii) après s'être assuré qu'un tel transfert est effectué conformément à la législation applicable. Cette interdiction s'applique également à l'assistance technique, à la maintenance et aux services similaires.

6. Audit et demande d'informations

6.1. Le Sous-Traitant informe sans délai le Responsable de Traitement de tout contact éventuel avec l'autorité de contrôle compétente ou une autre autorité en rapport avec le traitement de données à caractère personnel. Le Sous-Traitant n'est pas autorisé à représenter le Responsable de Traitement ou à agir de quelque manière que ce soit au nom du Responsable de Traitement vis-à-vis de l'autorité de contrôle compétente ou d'un tiers, sauf si le Responsable de Traitement a donné son accord écrit.

6.2. Le Sous-Traitant donne au Responsable de Traitement ou à un tiers autorisé par les Parties l'accès à toutes les informations non confidentielles nécessaires et requises pour permettre au Responsable de Traitement de vérifier et de contrôler le respect par le Sous-Traitant des obligations définies dans le présent DPA, le RGPD et tous autres lois applicables. Le Sous-Traitant doit également permettre et coopérer aux audits, y compris aux inspections, effectués par le Responsable de Traitement ou par un tiers mandaté par le Responsable de Traitement.

6.3. Le Sous-Traitant a le droit d'être indemnisé par le Responsable de Traitement afin de compenser les coûts directs raisonnables encourus par le Sous-Traitant à la suite d'un tel audit ou d'une telle inspection.

6.4. Le Sous-Traitant donne au Responsable de Traitement l'accès à toute information non confidentielle nécessaire et requise pour permettre au Responsable de Traitement de vérifier que les obligations découlant du présent DPA sont respectées et que le traitement est conforme aux exigences du droit applicable.

6.5. Dans les cas où une personne concernée, une autorité de contrôle compétente ou un autre tiers demande à l'une des Parties des informations sur des données à caractère personnel, les Parties coopèrent et échangent des informations dans la mesure nécessaire.

6.6. Le Sous-Traitant ne doit pas divulguer d'informations s'il n'a pas reçu le consentement écrit du Responsable de Traitement à cet effet ou si une telle obligation n'existe pas en vertu de la législation applicable ou sur ordre d'une autorité compétente.

7. Sous-Traitance ultérieure

7.1. Le Sous-Traitant ne doit pas sous-traiter le traitement de données à caractère personnel pour le compte du Responsable de Traitement sans informer le Responsable de Traitement par écrit, trente (30) jours avant une telle sous-traitance, de l'intention du Sous-Traitant de faire appel à un Sous-Traitant ultérieur.

7.2. Si le Sous-Traitant confie le traitement de données à caractère personnel à un Sous-Traitant ultérieur, il impose à ce dernier les mêmes obligations et contraintes que celles découlant du présent DPA. Le Sous-Traitant s'engage en outre à veiller à ce que le Sous-Traitant ultérieur respecte les dispositions des présentes conditions générales et à ce qu'il respecte également le droit applicable.

7.3. Lorsque le Sous-Traitant fait appel à un Sous-Traitant ultérieur conformément au présent DPA, il veille à ce que l'accord entre le Sous-Traitant et le Sous-Traitant ultérieur soit interprété de manière à ce que le Sous-Traitant ultérieur soit également lié par le présent DPA ainsi que par les exigences fixées dans le présent accord et par le droit applicable. Si le Sous-Traitant ultérieur ne remplit pas ses obligations, le Sous-Traitant est entièrement responsable vis-à-vis du Responsable de Traitement de l'exécution des obligations de ce Sous-Traitant ultérieur. Le Sous-Traitant tient de temps à autre une liste actualisée des Sous-Traitants ultérieurs qui peuvent être engagés. la demande du Responsable de Traitement, le Sous-Traitant fournit une copie de cette liste au Responsable de Traitement.

7.4. Le Responsable de Traitement ou une personne désignée par lui a le droit d'être assisté par le Sous-Traitant dans la réalisation d'une inspection ou d'un audit du traitement des données à caractère personnel par le Sous-Traitant ultérieur désigné.

8. Violation de données à caractère personnel

8.1. Dans le cas où le Sous-Traitant suspecte ou constate un type quelconque de violation de la sécurité, comme un accès non autorisé, une destruction, une modification de données à caractère personnel ou autre, ou si, pour une raison quelconque, le Sous-Traitant n'est pas en mesure de respecter les engagements et obligations prévus dans le présent DPA, le Sous-Traitant doit enquêter immédiatement sur l'incident et prendre les mesures appropriées pour y remédier et éviter que de tels événements ne se reproduisent.

8.2. Le Sous-Traitant informe le Responsable de Traitement dans les meilleurs délais après avoir pris connaissance d'une violation de données à caractère personnel et informe le Responsable de Traitement de cette violation de manière continue, dès que des informations sur la violation sont mises à sa disposition.

La notification doit contenir au moins les informations suivantes :

a) une description de la nature de la violation de données à caractère personnel, si possible les catégories et le nombre approximatif de personnes concernées ainsi que les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

b) indiquer le nom et les coordonnées du délégué à la protection des données ou d'autres points de contact auprès desquels des informations complémentaires peuvent être obtenues,

c) une description des conséquences probables de la violation de la protection des données à caractère personnel ; et

d) une description des mesures prises ou proposées par le Sous-Traitant pour remédier à la violation, y compris, le cas échéant, des mesures visant à en atténuer les effets négatifs potentiels.

8.3. Le Sous-Traitant doit informer le Responsable de Traitement sans délai lorsque

a) le Sous-Traitant a encore connaissance d'un traitement de données à caractère personnel qui est contraire aux instructions du Responsable de Traitement ou à le présent DPA ; et/ou

b) le Sous-Traitant estime qu'une instruction est contraire au droit applicable.

8.4. Lorsqu'un type particulier de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, notamment en ce qui concerne l'utilisation de nouvelles technologies et compte tenu de sa nature, de sa portée, de son contexte et de ses finalités, le Sous-Traitant doit, avant la mise en œuvre du traitement, aider le Responsable de Traitement à évaluer l'incidence prévue du traitement sur la protection des données à caractère personnel.

9. Responsabilité

9.1. L'article 82 du RGPD s'applique dans le cas où une personne concernée se voit accorder des dommages et intérêts par une décision de justice ou une autre décision en raison d'une violation d'une disposition du présent DPA, d'une instruction du Responsable de Traitement ou de la législation applicable en matière de protection des données.

9.2. Si une amende est infligée en vertu de l'article 83 du RGPD ou du droit national applicable, l'amende doit être payée par la partie qui reçoit cette amende.

9.3. Si une partie a connaissance d'un fait susceptible de causer un dommage à l'autre partie, elle en informe immédiatement cette dernière et coopère activement avec l'autre partie afin de prévenir ou de minimiser un tel dommage.

9.4. Nonobstant les indications figurant dans les TOSP des Parties et dans les annexes y afférentes, les sections 9.1. et 9.2. du DPA s'appliquent avant toute autre disposition relative à la cessation des obligations existant entre les parties en ce qui concerne le traitement des données à caractère personnel.

10. Indemnisation

10.1. Le Sous-Traitant n'a droit à aucune indemnisation pour les mesures qu'il prend dans le cadre du traitement des données à caractère personnel, sauf disposition contraire du présent DPA ou ddu contrat de revendeur conclu entre les Parties.

11. Durée

11.1. Le présent DPA entre en vigueur à la date de sa signature et s'applique aussi longtemps que le Sous-Traitant traite des données à caractère personnel dans le cadre des TOSP des parties.

12. Fin

12.1. Lorsque le Sous-Traitant cesse de traiter des données à caractère personnel pour le compte du Responsable de Traitement dans le cadre du présent DPA, il doit, au choix du Responsable de Traitement, détruire, effacer et/ou renvoyer au Responsable de Traitement toutes les données à caractère personnel liées au présent accord, conformément aux instructions du Responsable de Traitement, et veiller à ce qu'aucune donnée à caractère personnel ou copie de données à caractère personnel ne soit plus en possession du Sous-Traitant, sauf si la législation applicable ou des raisons financières, y compris fiscales, l'exigent.

12.2. Après la fin du présent DPA, le Sous-Traitant veille à ce que l'obligation visée au point 12.1 du DPA s'applique également à tous les Sous-Traitants ultérieurs.

13. Modifications

13.1. Le Responsable de Traitement peut modifier le contenu du DPA si cela est nécessaire pour se conformer au droit applicable. Une modification peut entrer en vigueur trente (30) jours après que le Responsable de Traitement a notifié la modification au Sous-Traitant. Si le Sous-Traitant n'accepte pas la modification en question, le Responsable de Traitement a le droit de résilier tous les contrats avec le Sous-Traitant en vertu desquels le Sous-Traitant doit traiter des données à caractère personnel.

13.2. Les avenants à ce DPA doivent être faits par écrit et signés par les deux parties afin d'être juridiquement contraignants.

14. Clauses contractuelles types

14.1. Dans le champ d'application de la décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil, les clauses contractuelles types (« **CCT** ») figurant à l'annexe 1 s'appliquent.

15. Dispositions applicables et ordre de priorité

15.1. Les accords entre les parties s'appliquent dans l'ordre suivant, étant entendu qu'en cas de contradiction, les dispositions des documents mentionnés en premier lieu prévalent sur les dispositions des documents mentionnés en second lieu :

a) CCT soumises au présent DPA, reproduites en Annexe 1 ;

b) les stipulations du présent DPA et

c) les stipulations des TOSP

16. Droit applicable et juridiction

16.1. Le présent DPA est soumis au droit _____ . Tout litige, tout désaccord ou toute réclamation découlant de ou en rapport avec la présente DPA, sont portées devant les juridictions générales de_____ définitivement, le tribunal d'instance de _____ est la première instance.

Le présent DPA peut être établi en un nombre indéterminé d'exemplaires, y compris sous forme électronique.

_____ Date

_____ Date

_____	_____
Signature du Responsable du Traitement	**Signature du Sous-Traitant**
_____	_____
Nom et titre en caractères d'imprimerie	Nom et titre en lettres d'imprimerie

ANNEXE 1 : CLAUSES CONTRACTUELLES TYPES

MODULE DEUX : Transfert des responsables du traitement aux Sous-Traitants

SECTION I

Clause 1

Finalités et champ d'application

(a) Les présentes clauses contractuelles types visent à garantir le respect des exigences du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)[1] en cas de transfert de données à caractère personnel vers un pays tiers.

(b) Les parties:

(i) la ou les personnes physiques ou morales, la ou les autorités publiques, la ou les agences ou autre(s) organisme(s) (ci-après la ou les «entités») qui transfèrent les données à caractère personnel, mentionnés à l'annexe I.A. (ci- après l'«exportateur de données»), et

(ii) la ou les entités d'un pays tiers qui reçoivent les données à caractère personnel de l'exportateur de données, directement ou indirectement par l'intermédiaire d'une autre entité également partie aux présentes clauses, mentionnées à l'annexe I.A. (ci-après l'«importateur de données»)

sont convenues des présentes clauses contractuelles types (ci-après les «clauses»).

(c) Les présentes clauses s'appliquent au transfert de données à caractère personnel précisé à l'annexe I.B.

(d) L'appendice aux présentes clauses, qui contient les annexes qui y sont mentionnées, fait partie intégrante des présentes clauses.

Clause 2

Effet et invariabilité des clauses

(a) Les présentes clauses établissent des garanties appropriées, notamment des droits opposables pour la personne concernée et des voies de droit effectives, en vertu de l'article 46, paragraphe 1, et de l'article 46, paragraphe 2, point c), du règlement (UE) 2016/679 et, en ce qui concerne les transferts de données de responsables du traitement à sous-traitants et/ou de sous-traitants à sous-traitants, des clauses contractuelles types en vertu de l'article 28, paragraphe 7, du règlement (UE) 2016/679, à condition qu'elles ne soient pas modifiées, sauf pour sélectionner le ou les modules appropriés ou pour ajouter ou mettre à jour des informations dans l'appendice. Cela n'empêche pas les parties d'inclure les clauses

[1] Si l'exportateur de données est un sous-traitant soumis au règlement (UE) 2016/679 agissant pour le compte d'une institution ou d'un organe de l'Union en tant que responsable du traitement, le recours aux présentes clauses lors du recrutement d'un autre sous-traitant (sous-traitance ultérieure) qui n'est pas soumis au règlement (UE) 2016/679 garantit également le respect de l'article 29, paragraphe 4, du règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39), dans la mesure où les présentes clauses et les obligations en matière de protection des données fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément à l'article 29, paragraphe 3, du règlement (UE) 2018/1725 sont alignées. Ce sera en particulier le cas lorsque le responsable du traitement et le sous-traitant se fondent sur les clauses contractuelles types qui figurent dans la décision […].

contractuelles types prévues dans les présentes clauses dans un contrat plus large et/ou d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les présentes clauses et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

(b) Les présentes clauses sont sans préjudice des obligations auxquelles l'exportateur de données est soumis en vertu du règlement (UE) 2016/679.

Clause 3

Tiers bénéficiaires

(a) Les personnes concernées peuvent invoquer et faire appliquer les présentes clauses, en tant que tiers bénéficiaires, contre l'exportateur et/ou l'importateur de données, avec les exceptions suivantes:

(i) clause 1, clause 2, clause 3, clause 6, clause 7;

(ii) clause 8 - module 1: clause 8.5, paragraphe e), et clause 8.9, paragraphe b);module 2: clause 8.1, paragraphe b), clause 8.9, paragraphes a), c), d) et e);module 3: clause 8.1, paragraphes a), c) et d) et clause 8.9, paragraphes a), c), d), e), f) et g); module 4: clause 8.1, paragraphe b), et clause 8.3,paragraphe b);

(iii) clause 9 - module 2: clause 9, paragraphes a), c), d) et e); module 3: clause 9,paragraphes a) c), d) et e);

(iv) clause 12 - module 1: clause 12, paragraphes a) et d); modules 2 et 3: clause 12, paragraphes a), d) et f);

(v) clause 13;

(vi) clause 15.1, paragraphes c), d) et e);

(vii) clause 16, paragraphe e);

(viii) clause 18 - modules 1, 2 et 3: clause 18, paragraphes a) et b); module 4:clause 18.

(b) Le paragraphe a) est sans préjudice des droits des personnes concernées au titre durèglement (UE) 2016/679.

Clause 4

Interprétation

(a) Lorsque les présentes clauses utilisent des termes définis dans le règlement(UE) 2016/679, ceux-ci ont la même signification que dans ledit règlement.

(b) Les présentes clauses sont lues et interprétées à la lumière des dispositions durèglement (UE) 2016/679.

(c) Les présentes clauses ne sont pas interprétées dans un sens contraire aux droits et obligations prévus dans le règlement (UE) 2016/679.

Clause 5

Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes entre les parties existant au moment où les présentes clauses sont convenues, ou souscrites parla suite, les présentes clauses prévalent.

Clause 6

Description du ou des transferts

Les détails du ou des transferts, en particulier les catégories de données à caractère personnel qui sont transférées et la ou les finalités pour lesquelles elles le sont, sont précisés à l'annexe I.B.

Clause 7 - Facultative

Clause d'adhésion

(a) Une entité qui n'est pas partie aux présentes clauses peut, avec l'accord des parties, yadhérer à tout moment, soit en tant qu'exportateur de données soit en tant qu'importateur de données, en remplissant l'appendice et en signant l'annexe I.A.

(b) Une fois l'appendice rempli et l'annexe I.A. signée, l'entité adhérente devient partie aux présentes clauses et a les droits et obligations d'un exportateur de données ou d'un importateur de données selon sa désignation dans l'annexe I.A.

(c) L'entité adhérente n'a aucun droit ni obligation découlant des présentes clauses pour la période antérieure à son adhésion à celles-ci.

SECTION II – OBLIGATIONS DES PARTIES

Clause 8

Garanties en matière de protection des données

L'exportateur de données garantit qu'il a entrepris des démarches raisonnables pour s'assurer que l'importateur de données est à même, par la mise en œuvre de mesures techniques et organisationnelles appropriées, de satisfaire aux obligations qui lui incombent en vertu des présentes clauses.

MODULE 2: transfert de responsable du traitement à sous-traitant

8.1 Instructions

(a) L'importateur de données ne traite les données à caractère personnel que sur instructions documentées de l'exportateur de données. L'exportateur de données peut donner ces instructions pendant toute la durée du contrat.

(b) S'il n'est pas en mesure de suivre ces instructions, l'importateur de données en informe immédiatement l'exportateur de données.

8.2 Limitation des finalités

L'importateur de données traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du transfert, telles que précisées à l'annexe I.B, sauf en cas d'instructions supplémentaires de l'exportateur de données.

8.3 Transparence

Sur demande, l'exportateur de données met gratuitement à la disposition de la personne concernée une copie des présentes clauses, notamment de l'appendice tel que rempli par les parties. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les mesures décrites à l'annexe II et les données à caractère personnel, l'exportateur de données peut occulter une partie du texte de l'appendice aux présentes clauses avant d'en communiquer une copie,

mais fournit un résumé valable s'il serait autrement impossible, pour la personne concernée, d'en comprendre le contenu ou d'exercer ses droits. Les parties fournissent à la personne concernée, à la demande de celle-ci, les motifs des occultations, dans la mesure du possible sans révéler les informations occultées.Cette clause est sans préjudice des obligations qui incombent à l'exportateur de données en vertu des articles 13 et 14 du règlement (UE) 2016/679.

8.4 Exactitude

Si l'importateur de données se rend compte que les données à caractère personnel qu'il a reçues sont inexactes, ou sont obsolètes, il en informe l'exportateur de données dans les meilleurs délais. Dans ce cas, l'importateur de données coopère avec l'exportateur de donnéespour effacer ou rectifier les données.

8.5 Durée du traitement et effacement ou restitution des données

Le traitement par l'importateur de données n'a lieu que pendant la durée précisée à l'annexe I.B. Au terme de la prestation des services de traitement, l'importateur de données, à la convenance de l'exportateur de données, efface toutes les données à caractère personnel traitées pour le compte de ce dernier et lui en apporte la preuve, ou lui restitue toutes les données à caractère personnel traitées pour son compte et efface les copies existantes. Jusqu'àce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement des données à caractère personnel, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données à caractère personnel que dans la mesure où et aussi longtemps que cette législation locale l'exige. Ceci est sans préjudice de la clause 14, en particulier de l'obligation imposée à l'importateur de données par la clause 14, paragraphe e), d'informer l'exportateur de données,pendant toute la durée du contrat, s'il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences de la clause 14,paragraphe a).

8.6 Sécurité du traitement

(a) L'importateur de données et, durant la transmission, l'exportateur de données mettent en œuvre des mesures techniques et organisationnelles appropriées pourgarantir la sécurité des données, notamment pour les protéger d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à ces données (ci-après la «violation de données à caractère personnel»). Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances,des coûts de mise en œuvre, de la nature, de la portée, du contexte et de la ou des finalités du traitement ainsi que des risques inhérents au traitement pour les personnes concernées. Les parties envisagent en particulier de recourir au chiffrement ou à la pseudonymisation, notamment pendant la transmission, lorsque lafinalité du traitement peut être atteinte de cette manière. En cas de pseudonymisation, les informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée précise restent, dans la mesure du possible, sous le contrôle exclusif de l'exportateur de données. Pour s'acquitter des obligations qui lui incombent en vertu du présent paragraphe, l'importateur de données met au moinsen œuvre les mesures techniques et organisationnelles précisées à l'annexe II. Il procède à des contrôles réguliers pour s'assurer que ces mesures continuent d'offrir le niveau de sécurité approprié.

(b) L'importateur de données ne donne l'accès aux données à caractère personnel aux membres de son personnel que dans la mesure strictement nécessaire à la mise en œuvre, à la gestion et au suivi du contrat. Il veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

(c) En cas de violation de données à caractère personnel concernant des données à caractère

personnel traitées par l'importateur de données au titre des présentes clauses, ce dernier prend des mesures appropriées pour remédier à la violation, y compris des mesures visant à en atténuer les effets négatifs. L'importateur de données informe également l'exportateur de données de cette violation dans lesmeilleurs délais après en avoir eu connaissance. Cette notification contient les coordonnées d'un point de contact auprès duquel il est possible d'obtenir plus d'informations, ainsi qu'une description de la nature de la violation (y compris, si possible, les catégories et le nombre approximatif de personnes concernées et d'enregistrements de données à caractère personnel concernés), de ses conséquences probables et des mesures prises ou proposées pour y remédier, y compris, le cas échéant, des mesures visant à en atténuer les effets négatifs potentiels. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et les autres informations sont fournies par la suite, dans les meilleurs délais, à mesure qu'elles deviennent disponibles.

(d) L'importateur de données coopère avec l'exportateur de données et l'aide afin de lui permettre de respecter les obligations qui lui incombent en vertu du règlement (UE) 2016/679, notamment celle d'informer l'autorité de contrôle compétente et les personnes concernées, compte tenu de la nature du traitement etdes informations à la disposition de l'importateur de données.

8.7 Données sensibles

Lorsque le transfert concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne, ou des données relatives àdes condamnations pénales et à des infractions (ci-après les «données sensibles»), l'importateur de données applique les restrictions particulières et/ou les garanties supplémentaires décrites à l'annexe I.B.

8.8 Transferts ultérieurs

L'importateur de données ne divulgue les données à caractère personnel à un tiers que sur instructions documentées de l'exportateur de données. En outre, les données ne peuvent être divulguées à un tiers situé en dehors de l'Union européenne[2] (dans le même pays quel'importateur de données ou dans un autre pays tiers, ci-après «transfert ultérieur»), que si le tiers est lié par les présentes clauses ou accepte de l'être, en vertu du module approprié, ou si:

(i) le transfert ultérieur est effectué vers un pays bénéficiant d'une décision d'adéquation en vertu de l'article 45 du règlement (UE) 2016/679 qui couvre letransfert ultérieur;

(ii) le tiers offre d'une autre manière des garanties appropriées conformément aux articles 46 ou 47 du règlement (UE) 2016/679 en ce qui concerne le traitement en question;

(iii) le transfert ultérieur est nécessaire à la constatation, à l'exercice ou à la défensed'un droit en justice dans le contexte de procédures administratives, réglementaires ou judiciaires spécifiques; ou

(iv) le transfert ultérieur est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Tout transfert ultérieur est soumis au respect, par l'importateur de données, de toutes les autres garanties au titre des présentes clauses, en particulier de la limitation des finalités.

[2] L'accord sur l'Espace économique européen (accord EEE) prévoit l'extension du marché intérieur de l'Union européenne aux trois pays de l'EEE que sont l'Islande, le Liechtenstein et la Norvège. La législation de l'Union en matière de protection des données, notamment le règlement (UE) 2016/679, est couverte par l'accord EEE et a été intégrée dans l'annexe XI de celui-ci. Dès lors, une divulgation par l'importateur de données à un tiers situé dans l'EEE ne peut être qualifiée de transfert ultérieur aux fins des présentes clauses.

8.9 Documentation et conformité

(a) L'importateur de données traite rapidement et de manière appropriée les demandes de renseignements de l'exportateur de données concernant le traitement au titre des présentes clauses.

(b) Les parties sont en mesure de démontrer le respect des présentes clauses. En particulier, l'importateur de données conserve une trace documentaire appropriée des activités de traitement menées pour le compte de l'exportateur de données.

(c) L'importateur de données met à la disposition de l'exportateur de données toutes les informations nécessaires pour démontrer le respect des obligations prévues par les présentes clauses et, à la demande de l'exportateur de données, pour permettre la réalisation d'audits des activités de traitement couvertes par les présentes clauses, et contribuer à ces audits, à intervalles raisonnables ou s'il existe des indications de non-respect. Lorsqu'il décide d'un examen ou d'un audit, l'exportateur de données peut tenir compte des certifications pertinentes détenues par l'importateur de données.

(d) L'exportateur de données peut choisir de procéder à l'audit lui-même ou de mandaterun auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques de l'importateur de données et sont, le cas échéant, effectués avec un préavis raisonnable.

(e) Les parties mettent à la disposition de l'autorité de contrôle compétente, à la demande de celle-ci, les informations mentionnées aux paragraphes b) et c), y compris les résultats de tout audit.

Clause 9

Recours à des sous-traitants ultérieurs

MODULE 2: transfert de responsable du traitement à sous-traitant

(a) OPTION 1: AUTORISATION PRÉALABLE SPÉCIFIQUE L'importateur de données ne sous-traite aucune des activités de traitement qu'il mène pour le compte de l'exportateur de données au titre des présentes clauses à un sous-traitant ultérieur sans l'autorisation écrite préalable spécifique de l'exportateur de données. L'importateur de données soumet la demande d'autorisation spécifique au moins [*précisez le délai*] avant le recrutement du sous-traitant ultérieur, avec les informations nécessaires pour permettre à l'exportateur de données de se prononcer sur l'autorisation. La liste des sous-traitants ultérieurs déjà autorisés par l'exportateurde données est disponible à l'annexe III. Les parties tiennent cette annexe à jour.

OPTION 2: AUTORISATION ÉCRITE GÉNÉRALE L'importateur de données a l'autorisation générale de l'exportateur de données de recruter un ou plusieurs sous- traitants ultérieurs à partir d'une liste arrêtée d'un commun accord. L'importateur de données informe expressément par écrit l'exportateur de données de tout changement concernant l'ajout ou le remplacement de sous-traitants ultérieurs qu'il est prévu d'apporter à cette liste au moins [*précisez le délai*] à l'avance, donnant ainsi à l'exportateur de données suffisamment de temps pour émettre des objections à l'encontre de ces changements avant le recrutement du ou des sous-traitants ultérieurs L'importateur de données fournit à l'exportateur de données les informations nécessaires pour permettre à ce dernier d'exercer son droit d'émettredes objections.

(b) Lorsque l'importateur de données recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte de l'exportateur de données), il le fait au moyen d'un

contrat écrit qui prévoit, en substance, les mêmes obligations en matière de protection des données que celles qui lient l'importateur de données au titre des présentes clauses, notamment en ce qui concerne les droits du tiers bénéficiaire pour les personnes concernées[3]. Les parties conviennent qu'en respectant la présente clause, l'importateur de données satisfait aux obligations qui lui incombent en vertu de la clause 8.8. L'importateur de données veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses.

(c) L'importateur de données fournit à l'exportateur de données, à la demande de celui- ci, une copie du contrat avec le sous-traitant ultérieur et de ses éventuelles modifications ultérieures. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les données à caractère personnel, l'importateur de données peut occulter une partie du texte du contrat avant d'en communiquer une copie.

(d) L'importateur de données reste pleinement responsable à l'égard de l'exportateur de données de l'exécution des obligations qui incombent au sous-traitant ultérieur en vertu du contrat qu'il a conclu avec lui. L'importateur de données notifie à l'exportateur de données tout manquement du sous-traitant ultérieur aux obligations qui lui incombent en vertu dudit contrat.

(e) L'importateur de données convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire en vertu de laquelle, dans les cas où l'importateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'exportateur de données a le droit de résilier le contrat du sous-traitant ultérieur et dedonner instruction à ce dernier d'effacer ou de restituer les données à caractère personnel.

Clause 10

Droits des personnes concernées

MODULE 2: transfert de responsable du traitement à sous-traitant

(a) L'importateur de données informe rapidement l'exportateur de données de toute demande reçue d'une personne concernée. Il ne répond pas lui-même à cette demande, à moins d'y avoir été autorisé par l'exportateur de données.

(b) L'importateur de données aide l'exportateur de données à s'acquitter de son obligation de répondre aux demandes de personnes concernées désireuses d'exercer leurs droits en vertu du règlement (UE) 2016/679. À cet égard, les parties indiquent àl'annexe II les mesures techniques et organisationnelles appropriées, compte tenu de la nature du traitement, au moyen desquelles l'aide sera fournie, ainsi que la portée etl'étendue de l'aide requise.

(c) Lorsqu'il s'acquitte des obligations qui lui incombent en vertu des paragraphes a)et b), l'importateur de données se conforme aux instructions de l'exportateur de données.

Clause 11

Voies de recours

(a) L'importateur de données informe les personnes concernées, sous une forme transparente et aisément accessible, au moyen d'une notification individuelle ou sur son site web, d'un point de contact autorisé à traiter les réclamations. Il traite sans délai toute réclamation reçue d'une personne concernée.

[OPTION: L'importateur de données convient que les personnes concernées peuvent

[3] Cette exigence peut être satisfaite par l'adhésion du sous-traitant ultérieur aux présentes clauses en vertu du module approprié, conformément à la clause 7.

également introduire, sans frais, une réclamation auprès d'un organe de règlementdes litiges indépendant[4]. Il informe les personnes concernées, de la manière indiquéeau paragraphe a), de ce mécanisme de recours et du fait qu'elles ne sont pas tenues d'y recourir ni de respecter une hiérarchie dans les recours.]

MODULE 2: transfert de responsable du traitement à sous-traitant

(b) En cas de litige entre une personne concernée et l'une des parties portant sur le respect des présentes clauses, cette partie met tout en œuvre pour parvenir à un règlement à l'amiable dans les meilleurs délais. Les parties se tiennent mutuellement informées de ces litiges et, s'il y a lieu, coopèrent pour les résoudre.

(c) Lorsque la personne concernée invoque un droit du tiers bénéficiaire en vertu de la clause 3, l'importateur de données accepte la décision de la personne concernée:

(i) d'introduire une réclamation auprès de l'autorité de contrôle de l'État membre dans lequel se trouve sa résidence habituelle ou son lieu de travail, ou auprèsde l'autorité de contrôle compétente au sens de la clause 13;

(ii) de renvoyer le litige devant les juridictions compétentes au sens de la clause 18.

Les parties acceptent que la personne concernée puisse être représentée par un organisme, une organisation ou une association à but non lucratif dans les conditions énoncées à l'article 80, paragraphe 1, du règlement (UE) 2016/679.

(d) L'importateur de données se conforme à une décision qui est contraignante en vertu du droit applicable de l'Union ou d'un État membre.

(e) L'importateur de données convient que le choix effectué par la personne concernéene remettra pas en cause le droit procédural et matériel de cette dernière d'obtenir réparation conformément à la législation applicable.

Clause 12

Responsabilité

MODULE 2: transfert de responsable du traitement à sous-traitant

(a) Chaque partie est responsable envers la ou les autres parties des dommages qu'elle cause à l'autre ou aux autres parties du fait d'un manquement aux présentes clauses.

(b) L'importateur de données est responsable à l'égard de la personne concernée, et la personne concernée a le droit d'obtenir réparation de tout dommage matériel oumoral qui lui est causé par l'importateur de données ou son sous-traitant ultérieur du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses.

(c) Nonobstant le paragraphe b), l'exportateur de données est responsable à l'égard de la personne concernée et celle-ci a le droit d'obtenir réparation de tout dommage matériel ou moral qui lui est causé par l'exportateur de données ou l'importateur de données (ou son sous-traitant ultérieur) du fait d'une violation des droits du tiers bénéficiaire prévus par les présentes clauses. Ceci est sans préjudice de la responsabilité de l'exportateur de données et, si l'exportateur de données est un sous-traitant agissant pour le compte d'un responsable du traitement, de la responsabilité de ce dernier au titre du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725, selon le cas.

[4] L'importateur de données ne peut proposer un règlement des litiges indépendant par une instance d'arbitrage que s'il est établi dans un pays qui a ratifié la convention de New York pour la reconnaissance et l'exécution des sentences arbitrales étrangères.

(d) Les parties conviennent que, si l'exportateur de données est reconnu responsable, en vertu du paragraphe c), du dommage causé par l'importateur de données (ou son sous-traitant ultérieur), il a le droit de réclamer auprès de l'importateur de données la part de la réparation correspondant à la responsabilité de celui-ci dans le dommage.

(e) Lorsque plusieurs parties sont responsables d'un dommage causé à la personneconcernée du fait d'une violation des présentes clauses, toutes les parties responsables le sont conjointement et solidairement et la personne concernée a ledroit d'intenter une action en justice contre n'importe laquelle de ces parties.

(f) Les parties conviennent que, si la responsabilité d'une d'entre elles est reconnue en vertu du paragraphe e), celle-ci a le droit de réclamer auprès de l'autre ou des autres parties la part de la réparation correspondant à sa/leur responsabilité dans le dommage.

(g) L'importateur de données ne peut invoquer le comportement d'un sous-traitant ultérieur pour échapper à sa propre responsabilité.

Clause 13

Contrôle

MODULE 2: transfert de responsable du traitement à sous-traitant

(a) [Si l'exportateur de données est établi dans un État membre de l'Union:] L'autoritéde contrôle chargée de garantir le respect, par l'exportateur de données, du règlement (UE) 2016/679 en ce qui concerne le transfert de données, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité de contrôle compétente.

[Si l'exportateur de données n'est pas établi dans un État membre de l'Union, mais relève du champ d'application territorial du règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2, et a désigné un représentant en vertu de l'article 27, paragraphe 1, dudit règlement:] L'autorité de contrôle de l'État membre dans lequelle représentant au sens de l'article 27, paragraphe 1, du règlement (UE) 2016/679 est établi, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité de contrôle compétente.

[Si l'exportateur de données n'est pas établi dans un État membre de l'Union, mais relève du champ d'application territorial du règlement (UE) 2016/679 en vertu de son article 3, paragraphe 2 sans toutefois avoir à désigner un représentant en vertu de l'article 27, paragraphe 2, du règlement (UE) 2016/679:] L'autorité de contrôle d'un des États membres dans lesquels se trouvent les personnes concernées dont lesdonnées à caractère personnel sont transférées au titre des présentes clauses en lien avec l'offre de biens ou de services ou dont le comportement fait l'objet d'un suivi, telle qu'indiquée à l'annexe I.C, agit en qualité d'autorité compétente.

(b) L'importateur de données accepte de se soumettre à la juridiction de l'autorité de contrôle compétente et de coopérer avec elle dans le cadre de toute procédure visantà garantir le respect des présentes clauses. En particulier, l'importateur de données accepte de répondre aux demandes de renseignements, de se soumettre à des audits etde se conformer aux mesures adoptées par l'autorité de contrôle, notamment aux mesures correctrices et compensatoires. Il confirme par écrit à l'autorité de contrôle que les mesures nécessaires ont été prises.

SECTION III – LÉGISLATIONS LOCALES ET OBLIGATIONS EN CAS D'ACCÈSDES AUTORITÉS PUBLIQUES

Clause 14

Législations et pratiques locales ayant une incidence sur le respect des clauses

MODULE 2: transfert de responsable du traitement à sous-traitant

(a) Les parties garantissent qu'elles n'ont aucune raison de croire que la législation et lespratiques du pays tiers de destination applicables au traitement des données à caractère personnel par l'importateur de données, notamment les exigences en matière de divulgation de données à caractère personnel ou les mesures autorisant l'accès des autorités publiques à ces données, empêchent l'importateur de données des'acquitter des obligations qui lui incombent en vertu des présentes clauses. Cette disposition repose sur l'idée que les législations et les pratiques qui respectent l'essence des libertés et droits fondamentaux et qui n'excèdent pas ce qui est nécessaire et proportionné dans une société démocratique pour préserver un des objectifs énumérés à l'article 23, paragraphe 1, du règlement (UE) 2016/679 ne sont pas en contradiction avec les présentes clauses.

(b) Les parties déclarent qu'en fournissant la garantie mentionnée au paragraphe a), ellesont dûment tenu compte, en particulier, des éléments suivants:

(i) des circonstances particulières du transfert, parmi lesquelles la longueur de la chaîne de traitement, le nombre d'acteurs concernés et les canaux de transmission utilisés; les transferts ultérieurs prévus; le type de destinataire; la finalité du traitement; les catégories et le format des données à caractère

personnel transférées; le secteur économique dans lequel le transfert a lieu et le lieu de stockage des données transférées;

(ii) des législations et des pratiques du pays tiers de destination – notamment cellesqui exigent la divulgation de données aux autorités publiques ou qui autorisent l'accès de ces dernières aux données – pertinentes au regard des circonstances particulières du transfert, ainsi que des limitations et des garanties applicables[12];

(iii) de toute garantie contractuelle, technique ou organisationnelle pertinente mise en place pour compléter les garanties prévues par les présentes clauses, ycompris les mesures appliquées pendant la transmission et au traitement des données à caractère personnel dans le pays de destination.

(c) L'importateur de données garantit que, lors de l'évaluation au titre du paragraphe b), il a déployé tous les efforts possibles pour fournir des informations pertinentes à l'exportateur de données et convient qu'il continuera à coopérer avec ce dernier pour garantir le respect des présentes clauses.

(d) Les parties conviennent de conserver une trace documentaire de l'évaluation au titre du paragraphe b) et de mettre cette évaluation à la disposition de l'autorité de contrôle compétente si celle-ci en fait la demande.

(e) L'importateur de données accepte d'informer sans délai l'exportateur de données si, après avoir souscrit aux présentes clauses et pendant la durée du contrat, il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences du paragraphe a), notamment à la suite d'une modification de la législation du pays tiers ou d'une mesure (telle qu'une demande de divulgation) indiquant une application pratique de cette législation qui n'est pas conforme aux exigences du paragraphe a).

(f) À la suite d'une notification au titre du paragraphe e), ou si l'exportateur de donnéesa d'autres raisons de croire que l'importateur de données ne peut plus s'acquitter des obligations qui lui incombent en vertu des présentes clauses, l'exportateur de données définit sans délai les mesures appropriées (par exemple des mesures techniques ou organisationnelles visant à garantir la sécurité et la confidentialité) qu'il doit adopter et/ou qui doivent être adoptées par l'importateur de données pour remédier à la situation. L'exportateur de données suspend le transfert de donnéess'il estime qu'aucune garantie appropriée ne peut être fournie pour ce transfert ou si

---

[12] En ce qui concerne l'incidence de ces législations et pratiques sur le respect des présentes clauses, différents éléments peuvent être considérés comme faisant partie d'une évaluation globale. Ces éléments peuvent inclure une expérience concrète, documentée et pertinente de cas antérieurs de demandes de divulgation émanant d'autorités publiques, ou l'absence de telles demandes, couvrant un laps de temps suffisamment représentatif. Il peut s'agir de registres internes ou d'autres documents établis de manière continue conformément au principe de diligence raisonnable et certifiés à un niveau hiérarchique élevé, pour autantque ces informations puissent être partagées légalement avec des tiers. Lorsque cette expérience pratique est invoquée pour conclure que l'importateur de données ne sera pas empêché de respecter les présentes clauses, il y a lieu de l'étayer par d'autres éléments pertinents et objectifs, et il appartient aux parties d'examiner avec soin si ces éléments, pris dans leur ensemble, ont un poids suffisant, du point de vue de leur fiabilité et deleur représentativité, pour soutenir cette conclusion. En particulier, les parties doivent s'assurer que leur expérience pratique est corroborée et non contredite par des informations fiables accessibles au public ou disponibles d'une autre manière sur l'existence ou l'absence de demandes dans le même secteur et/ou sur l'application pratique du droit, comme la jurisprudence et les rapports d'organes de contrôle indépendants.

l'autorité de contrôle compétente lui en donne l'instruction. Dans ce cas, l'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement dedonnées à caractère personnel au titre des présentes clauses. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement. Lorsque le contrat est résilié en vertu de la présente clause, la clause 16, paragraphes d) et e), s'applique.

Clause 15

Obligations de l'importateur de données en cas d'accès des autorités publiques

MODULE 2: transfert de responsable du traitement à sous-traitant

15.1 Notification

(a) L'importateur de données convient d'informer sans délai l'exportateur de données et, si possible, la personne concernée (si nécessaire avec l'aide de l'exportateur de données):

(i) s'il reçoit une demande juridiquement contraignante d'une autorité publique, y compris judiciaire, en vertu de la législation du pays de destination en vue de ladivulgation de données à caractère personnel transférées au titre des présentes clauses; cette notification comprend des informations sur les données à caractère personnel demandées, l'autorité requérante, la base juridique de la demande et la réponse fournie; ou

(ii) s'il a connaissance d'un quelconque accès direct des autorités publiques aux données à caractère personnel transférées au titre des présentes clauses en vertude la législation du pays de destination; cette notification comprend toutes les informations dont l'importateur de données dispose.

(b) Si la législation du pays de destination interdit à l'importateur de données d'informer l'exportateur de données et/ou la personne concernée, l'importateur de données convient de tout mettre en œuvre pour obtenir une levée de cette interdiction, en vue de communiquer autant d'informations que possible, dans les meilleurs délais. L'importateur de données accepte de garder une trace documentaire des efforts qu'ila déployés afin de pouvoir en apporter la preuve à l'exportateur de données, si celui- ci lui en fait la demande.

(c) Lorsque la législation du pays de destination le permet, l'importateur de données accepte de fournir à l'exportateur de données, à intervalles réguliers pendant la durée

du contrat, autant d'informations utiles que possible sur les demandes reçues (notamment le nombre de demandes, le type de données demandées, la ou les autorités requérantes, la contestation ou non des demandes et l'issue de ces contestations, etc.).

(d) L'importateur de données accepte de conserver les informations mentionnées aux paragraphes a) à c) pendant la durée du contrat et de les mettre à la disposition de l'autorité de contrôle compétente si celle-ci lui en fait la demande.

(e) Les paragraphes a) à c) sont sans préjudice de l'obligation incombant à l'importateur de données, en vertu de la clause 14, paragraphe e), et de la clause 16, d'informer sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentesclauses.

15.2 Contrôle de la légalité et minimisation des données

(a) L'importateur de données accepte de contrôler la légalité de la demande de divulgation, en particulier de vérifier si elle s'inscrit dans les limites des pouvoirs conférés à l'autorité publique requérante, et de la contester si, après une évaluation minutieuse, il conclut qu'il existe des motifs raisonnables de considérer qu'elle est illégale en vertu de la législation du pays de destination, des obligations applicables en vertu du droit international et des principes de courtoisie internationale. L'importateur de données exerce les possibilités d'appel ultérieures dans les mêmes conditions. Lorsqu'il conteste une demande, l'importateur de données demande des mesures provisoires visant à suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente se prononce sur son bien-fondé. Il ne divulgue pas les données à caractère personnel demandées tant qu'il n'est pas obligé de le faire en vertu des règles de procédure applicables. Ces exigences sont sans préjudice des obligations incombant à l'importateur de données en vertu de la clause 14, paragraphe e).

(b) L'importateur de données accepte de garder une trace documentaire de son évaluation juridique ainsi que de toute contestation de la demande de divulgation et, dans la mesure où la législation du pays de destination le permet, de mettre les documents concernés à la disposition de l'exportateur de données. Il les met également à la disposition de l'autorité de contrôle compétente si celle-ci lui en faitla demande.

(c) L'importateur de données accepte de fournir le minimum d'informations autorisé lorsqu'il répond à une demande de divulgation, sur la base d'une interprétationraisonnable de la demande.

SECTION IV — DISPOSITIONS FINALES

Clause 16

Non-respect des clauses et résiliation

(a) L'importateur de données informe sans délai l'exportateur de données s'il n'est pas en mesure de respecter les présentes clauses, quelle qu'en soit la raison.

(b) Dans le cas où l'importateur de données enfreint les présentes clauses ou

n'est pas enmesure de les respecter, l'exportateur de données suspend le transfert de données à caractère personnel à l'importateur de données jusqu'à ce que le respect des présentes clauses soit à nouveau garanti ou que le contrat soit résilié. Ceci est sans préjudice de la clause 14, paragraphe f).

(c) L'exportateur de données a le droit de résilier le contrat, dans la mesure où il concerne le traitement de données à caractère personnel au titre des présentes clauses, lorsque:

(i) l'exportateur de données a suspendu le transfert de données à caractère personnel à l'importateur de données en vertu du paragraphe b) et que lerespect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension;

(ii) l'importateur de données enfreint gravement ou de manière persistante lesprésentes clauses; ou

(iii) l'importateur de données ne se conforme pas à une décision contraignante d'une juridiction ou d'une autorité de contrôle compétente concernant les obligations qui lui incombent au titre des présentes clauses.

Dans ces cas, il informe l'autorité de contrôle compétente de ce non-respect. Si le contrat concerne plus de deux parties, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en soient convenues autrement.

(d) [Pour les modules 1, 2 et 3: Les données à caractère personnel qui ont été transférées avant la résiliation du contrat au titre du paragraphe c) sont immédiatement restituéesà l'exportateur de données ou effacées dans leur intégralité, à la convenance de celui-ci. Il en va de même pour toute copie des données.] L'importateur de données apporte la preuve de l'effacement des données à l'exportateur de données. Jusqu'à ce que les données soient effacées ou restituées, l'importateur de données continue de veiller au respect des présentes clauses. Lorsque la législation locale applicable à l'importateur de données interdit la restitution ou l'effacement desdonnées à caractère personnel transférées, ce dernier garantit qu'il continuera à respecter les présentes clauses et qu'il ne traitera les données que dans la mesure oùet aussi longtemps que cette législation locale l'exige.

(e) Chaque partie peut révoquer son consentement à être liée par les présentes clauses i) si la Commission européenne adopte une décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 qui couvre le transfert de données à caractère personnel auquel les présentes clauses s'appliquent; ou ii) si le règlement (UE) 2016/679 est intégré dans le cadre juridique du pays vers lequel les données à caractère personnel sont transférées. Ceci est sans préjudice des autres obligations qui s'appliquent au traitement en question en vertu du règlement (UE) 2016/679.

Clause 17

Droit applicable

MODULE 2: transfert de responsable du traitement à sous-traitant

[OPTION 1: Les présentes clauses sont régies par le droit d'un des États membres de l'Union européenne, pour autant que ce droit reconnaisse des droits au tiers

bénéficiaire. Les parties conviennent qu'il s'agit du droit de/du/de la_(*précisez l'État membre*).]

[OPTION 2 (pour les modules 2 et 3): Les présentes clauses sont régies par le droit de l'État membre de l'Union européenne dans lequel l'exportateur de données est établi. Si ce droit ne reconnaît pas de droits au tiers bénéficiaire, les clauses sont régies par le droit d'un autre État membre de l'Union européenne qui reconnaît de tels droits. Les parties conviennent qu'il s'agit du droit de/du/de la_____(*précisez l'État membre*).]

Clause 18

Élection de for et juridiction

MODULE 2: transfert de responsable du traitement à sous-traitant

(a) Tout litige survenant du fait des présentes clauses est tranché par les juridictions d'unÉtat membre de l'Union européenne.

(b) Les parties conviennent qu'il s'agit des juridictions de/du/de la (*précisez l'État membre*).

(c) La personne concernée peut également poursuivre l'exportateur et/ou l'importateur de données devant les juridictions de l'État membre dans lequel elle a sa résidence habituelle.

(d) Les parties acceptent de se soumettre à la compétence de ces juridictions.

APPENDICE relative aux clauses contractuelles types

ANNEXE I

MODULE 2: transfert de responsable du traitement à sous-traitant

A. LISTE DES PARTIES

Exportateur(s) de données: *[Identité et coordonnées du ou des exportateurs de données et, le cas échéant, de leur délégué à la protection des données et/ou de leur représentant dans l'Union européenne]*

Nom :	
Adresse :	
Nom, fonction et coordonnées de la personne de contact :	
Activités en rapport avec les données transférées au titre des présentes clauses	
Signature et date :	
Rôle (responsable du traitement/sous-traitant) :	

Importateur(s) de données : [*nom et coordonnées de l'exportateur ou des importateurs de données, y compris la personne de contact responsable de la protection des données]*

Nom :	SMART Technologies ULC
Adresse :	Suite 600, 214 11 Avenue SW, Calgary, AB, Canada T2R 0K1
Nom, fonction et coordonnées de la personne de contact :	
Activités en rapport avec les données transférées au titre des présentes clauses	Traitement des données pour
Signature et date :	

Rôle (responsable du traitement/sous-traitant)	Sous-Traitant

B. DESCRIPTION DU TRANSFERT DE DONNÉES

Catégories de personnes concernées dont les données à caractère personnel sont transférées

- Utilisateur final
- Clients

Catégories de données à caractère personnel transmises

1. Utilisateur final

- Informations d'identification directes (par exemple, nom, adresse électronique)
- Toutes les données à caractère personnel fournies par les utilisateurs finaux du service
- Technique d'application Métadonnées
    - Adresses IP, utilisation de cookies, etc.
- Statistiques d'utilisation des applications
    - Métadonnées relatives à l'interaction de l'utilisateur avec l'application
    - Autres dates d'évaluation - définies par l'enseignant qui dirige la classe
- Communication en ligne saisie (e-mails, entrées de blog)
- Numéro d'identification de l'élève attribué au fournisseur d'accès/à l'application
- Nom d'utilisateur pour les applications pour les élèves
- Réponses des élèves à des enquêtes ou des questionnaires
- Contenus créés par les élèves : textes, images, etc. - tout ce qui est stocké dans le fichier de cours de l'enseignant
- Signature unique Microsoft
- Authentification unique Google
- Région de stockage des données (États-Unis ou UE)
- Google Analytics (anonyme)
- MixPanel-Analytics (anonyme)

2. Catégories de personnes concernées du Client

- Nom de l'organisation
- Courrier électronique
- Téléphone
- Adresse
- Informations requises pour la commande : Produit, quantité, prix et taxe, livraison

Les données sensibles transférées (le cas échéant) et les restrictions ou garanties appliquées, qui tiennent pleinement compte de la nature des données et des risques associés, telles qu'une stricte limitation des finalités, des restrictions d'accès (y compris l'accès réservé au personnel ayant suivi une formation spécifique), l'enregistrement de l'accès aux données, des restrictions sur les transferts ultérieurs ou des mesures de sécurité supplémentaires

Par les présentes, le Sous-Traitant interdit expressément au Responsable de Traitement de lui communiquer des catégories particulières de données à caractère personnel.

Fréquence de transmission (par exemple, si les données sont transmises une seule fois ou en continu)

En continu pendant l'utilisation du service.

Nature du traitement

Le Sous-Traitant effectuera les activités de traitement de base suivantes :

- Traitement visant à fournir le service conformément aux conditions des TOSP ;
- Traitement pour effectuer les démarches nécessaires à la fourniture du service ; et
- Traitement pour se conformer à d'autres instructions raisonnables du Responsable de Traitement (par exemple, par courrier électronique), qui sont conformes aux conditions des TOSP.

Finalité(s) du transfert et du traitement ultérieur des données

Le Sous-Traitant traite les données personnelles transmises, stockées ou envoyées via SMART Learning Suite afin de fournir le service et l'assistance technique associée conformément au présent DPA.

Durée de conservation des données à caractère personnel ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée

Pendant toute la durée du contrat de services ainsi que pendant la période suivant son expiration jusqu'à l'effacement des données à caractère personnel par le Sous-Traitant conformément à la législation applicable ou à la demande du Responsable de Traitement (demande d'effacement des données).

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

Indiquez la ou les autorités de contrôle compétentes conformément à la clause 13

……

~~**Note : si le Responsable de Traitement agit en tant qu'exportateur de données et est établi dans un État*~~ *membre de l'UE, l'autorité de contrôle chargée d'assurer le respect du règlement (UE) 2016/679 par l'exportateur de données en ce qui concerne le transfert de données, comme indiqué ici, agit en tant qu'autorité de contrôle compétente.*

ANNEXE II - MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS LES MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À GARANTIR LA SÉCURITÉ DES DONNÉES

MODULE 2: transfert de responsable du traitement à sous-traitant

Description des mesures techniques et organisationnelles mises en œuvre par le ou les importateurs de données (y compris toute certification pertinente) pour garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

Les parties conviennent de mettre en œuvre les catégories d'actions suivantes. Le détail de chaque action est disponible sur demande.

1. Le Sous-Traitant devrait disposer d'une organisation structurée dans laquelle les tâches et les responsabilités des différents membres du personnel en matière d'informations sur la sécurité sont clairement définies
2. Le Sous-Traitant propose régulièrement des cours de sensibilisation à la résilience des systèmes d'information.
3. Le Sous-Traitant doit disposer de routines et de fonctions lui permettant de supprimer et de détruire de manière permanente les informations ayant un lien avec la prestation.
4. le Sous-Traitant a procédé à une évaluation des risques du système et a pris des mesures afin d'identifier les éventuelles défaillances de ce système
5. Les exigences du Responsable de Traitement en matière de traitement des informations doivent être reprises. Si de telles exigences ne sont pas formulées, le Sous-Traitant doit être en mesure d'exposer les routines qui lui sont applicables.
6. Les utilisateurs doivent être dotés d'identités d'utilisateur personnelles et uniques, de sorte que les comptes d'invité anonymes ne peuvent pas être utilisés. Pour plus d'informations, consultez le guide du niveau de confiance 1 (LoA1).
7. Le Sous-Traitant doit respecter une routine convenue qui permet au Responsable de Traitement d'autoriser certains droits.
8. Le Sous-Traitant utilise des identités d'utilisateur personnelles et traçables pour des comptes dotés de droits plus étendus, utilisés pour gérer le système.
9. Le Sous-Traitant doit disposer d'un système permettant de distribuer et de réinitialiser les mots de passe sans que le mot de passe ne soit divulgué à des personnes non autorisées. Pour plus d'informations, consultez le guide du niveau de confiance 1 (LoA1).
10. Le système d'autorisation consigne des informations sur le moment où un utilisateur est créé ou supprimé.
11. Le Sous-Traitant doit disposer d'une routine pour supprimer les identités des utilisateurs du système.
12. Le Sous-Traitant doit avoir défini des règles pour la personne Responsable de Traitement des informations d'authentification.

13. Seules les informations ou les services qui sont publics peuvent être disponibles dans le système et dans toute autre infrastructure associée qui n'a pas fait l'objet d'une authentification.
14. Le système doit utiliser des mots de passe pour l'authentification ou tout autre moyen offrant un niveau de sécurité plus élevé. Des règles doivent être établies concernant la manière dont un mot de passe peut être géré dans le système et par un utilisateur. Pour plus d'informations, consultez le guide du niveau de confiance 1 (LoA1).
15. Ce que l'on appelle le data hall doit répondre au moins au niveau de protection 2 (correspondant à la "data room", appelée "Guidance for physical security information in the it-room" par l'agence suédoise de protection civile).
16. Le Sous-Traitant doit disposer de routines garantissant que seul le personnel autorisé a un accès physique à la "salle des données".
17. Le Sous-Traitant doit disposer de différentes fonctions, processus et routines pour surveiller les performances et faire des prévisions.
18. Le Sous-Traitant doit protéger les pièces incluses dans la livraison contre tout endommagement.
19. Le Sous-Traitant devrait disposer de routines et de fonctions de sauvegarde et de restauration des informations conformément aux exigences d'accessibilité convenues avec le responsable. Les sauvegardes devraient être protégées de la même manière que les informations originales et être conservées séparément.
20. Des fonctions de connexion devraient être disponibles pour les événements liés à la sécurité, notamment les connexions erronées, toute modification d'une autorisation, les connexions non autorisées et les violations d'autorisation.
21. Le Sous-Traitant protège les fonctions de connexion et les outils de journalisation contre les manipulations et les accès non autorisés, y compris par les employés du Sous-Traitant.
22. Le système et l'infrastructure associée doivent utiliser la même synchronisation horaire que la source de temps, c'est-à-dire UTC+0.
23. Le Sous-Traitant informe immédiatement le Responsable de Traitement des vulnérabilités techniques des composants livrés. Les points faibles découverts doivent être éliminés sans délai.
24. Le responsable est informé, sur demande, de tout échange d'informations avec d'autres systèmes en dehors de l'environnement du client.
25. Le Sous-Traitant a défini et documenté des principes et des méthodes pour le développement de systèmes sûrs et les présente au Responsable de Traitement.
26. Le Sous-Traitant a des directives pour un système d'information qu'il respecte dans le cadre de ses processus de développement.
27. Les responsabilités du Sous-Traitant mentionnées ici s'appliquent à tous les Sous-Traitants. Le responsable doit être informé, sur demande, du Sous-Traitant ultérieur auquel il est fait appel.

28. Le Sous-Traitant doit disposer de routines pour la notification, l'escalade et le traitement des événements ou incidents de sécurité.
29. Le Sous-Traitant coopère avec un organisme désigné par le Responsable de Traitement pour traiter les vulnérabilités, les événements de sécurité ou les incidents.
30. Le Sous-Traitant s'efforcera en permanence, en collaboration avec le Responsable de Traitement, de veiller à ce que la livraison respecte toutes les lois, réglementations et règles pertinentes applicables à l'activité du Responsable de Traitement.
31. En cas de traitement de données à caractère personnel, le Responsable de Traitement doit conclure un accord de traitement avec le Sous-Traitant avant que le contrat ne prenne effet.
32. Le Sous-Traitant doit obtenir une autorisation avant de réutiliser les informations contenues dans le système (textes, images, etc.) dans un autre contexte.

ANNEXE III - LISTE DES SOUS-TRAITANTS ULTERIEURS

LISTE DES SOUS-TRAITANTS (*source :* https://www.smarttech.com/lumio/legal/privacy)

Le Responsable de Traitement a autorisé le recours aux Sous-Traitants suivants :

INVITÉS

Nom d'affichage choisi par l'invité

Où	Qui	Données et finalités
Canada	SMART Technologies ULC	Nécessaire pour les fonctionnalités de base. Le nom d'affichage est indiqué dans leçon ou activité d'un enseignant enregistrée lorsque l'utilisateur y participe.
		SLS Terms (Conditions générales de vente SLS) RGPD - Décision d'adéquation de la Commission
Etats-Unis / Allemagne	Amazon Web Services, Inc.	Nécessaire pour le stockage. Nous proposons à la fois une option de stockage des données américaine et européenne. AWS Privacy (Foire aux questions sur la protection des données) AWS GPDR (Centre du Règlement général sur la protection des données
États-Unis/ Belgique	Firebase (Google LLC)	Nécessaire pour la fonctionnalité de base (Firebase est une solution de cloud computing backend-as-a-service (BaaS) que nous utilisons pour le traitement informatique automatisé (temporaire) en temps réel). Firebase Privacy (protection des données et sécurité dans Firebase) Firebase RGPD (protection des données

Contenu créé par les invités

Où	Qui	Données et finalité
Canada	SMART Technologies ULC	Facultatif (*enregistré dans le cours de l'enseignant*) SLS Terms (Conditions générales de vente SLS) RGPD - Décision d'adéquation de la CE Commission

Etats-Unis/ Allemagne	Amazon Web Services, Inc	Nécessaire pour le stockage. Nous proposons à la fois un site américain ainsi qu'une option européenne de stockage des données. AWS Privacy (Foire aux questions sur la protection des données) AWS GPDR (Centre du Règlement général sur la protection des données (RGPD))
Etats-Unis / Belgique	Firebase (Google LLC)	Nécessaire pour la fonctionnalité de base (Firebase est une solution de cloud computing backend-as-a-service (BaaS) que nous utilisons pour le traitement informatique automatisé (temporaire) en temps réel). Firebase Privacy (protection des données et sécurité dans Firebase) Firebase RGPD (protection des données

Analyse des invités

Où	**Qui**	**Données et finalité**
Canada	SMART Technologies ULC	Nécessaire pour l'amélioration des produits et le suivi des services. Nous utilisons Mixpanel en tant que notre Sous-traitant à ces fins. SLS Terms (Conditions générales de vente SLS) RGPD - Décision d'adéquation de la Commission européenne
USA	Mixpanel, Inc.	Nécessaire pour l'amélioration des produits et le suivi des services. Nous analysons comment nos utilisateurs non identifiés interagissent avec Lumio. Cela sert à identifier des tendances, à comprendre le comportement général agrégé des utilisateurs et à nous aider à prendre de meilleures décisions sur la manière d'améliorer l'expérience utilisateur et les fonctionnalités de notre produit. Ces données sont également utilisées pour suivre le temps nécessaire à nos serveurs pour terminer des actions telles que l'ouverture de fichiers, ce qui nous aide à mesurer l'état du service et le temps de montée/descente.

		Mixpanel Privacy (Informations sur la protection des données) Mixpanel RGPD
N/A	Tiers	Contenu ou activités optionnels qu'un enseignant ajoute à une leçon, comme par exemple YouTube ou tout autre contenu intégré qu'un utilisateur ajoute volontairement. Le contenu ne peut pas contrôler les données directement collectées par un tiers lorsqu'un enseignant ou un élève décide de les inclure dans une leçon. Cependant, pour le contenu premium que SMART met à disposition, nous ne signalons que l'utilisation anonyme au fournisseur tiers.
États-Unis	Sentry.io	ID de la leçon (aucune donnée personnelle) • ID d'utilisateur et ID de session (hachés et dotés de ce que l'on appelle un salt pour préserver l'anonymat) • En-tête de la requête (application et version, plate-forme, système d'exploitation, navigateur, langue, date et heure) • Bread crumbs (dernières pages visitées et liens cliqués) • Rapport d'erreur facultatif par l'utilisateur : une fois que le message d'erreur automatique est terminé, les utilisateurs ont la possibilité d'indiquer leur nom, leur adresse électronique et des informations supplémentaires sur l'erreur. Il est également demandé aux utilisateurs s'ils souhaitent que SMART les contacte. Ces informations personnelles facultatives sont stockées dans Salesforce (aux États-Unis) et transmises à notre équipe de service clientèle. Sentry Confidentialité Sentry RGPD

Etats-Unis	Slack Technologies LLC	• ID de la leçon (pas de données personnelles) • ID d'utilisateur et ID de session (hachés et salés pour préserver l'anonymat) • En-tête de la requête (application et version, plate-forme, système d'exploitation, navigateur, langue, date et heure) • Breadcrumbs (dernières pages visitées et liens cliqués) Rapport d'auto-échec facultatif : une fois que le rapport d'auto-échec automatique est terminée, les utilisateurs ont la possibilité d'indiquer leur nom, leur adresse électronique et des informations supplémentaires sur l'erreur. Il est également demandé aux utilisateurs s'ils souhaitent que SMART les contacte. Ces données personnelles facultatives sont stockées dans Salesforce (basé aux États-Unis) et partagées avec nos équipes d'assistance clientèle et de développement via Sentry et Slack. Confidentialité Slack Slack RGPD
USA	Splunk Inc.	Métadonnées requises, y compris les journaux système et les performances. Splunk Protection de la vie privée Splunk RGPD

ÉLÈVES / MINEURS, INSCRITS

Compte d'étudiant

Où	**Qui**	**Données et finalités**
Canada	SMART Technoloies ULC	Données de compte requises pour la fonctionnalité du produit : Nom d'affichage, nom complet, e-mail, photo de profil public, langue préférée SLS Terms (Conditions générales de vente SLS) RGPD - Décision d'adéquation de la CE Commission
Global	Microsoft, Inc.	Obligatoire si vous utilisez Microsoft en tant que fournisseur de signature unique (SSO).pour accéder à Lumio. Microsoft fournit à SMART les informations de compte nécessaires. Microsoft SSO Protection des données Microsoft Microsoft RGPD

Global	Google LLC	Obligatoire si vous utilisez Google en tant que fournisseur d'authentification unique (SSO) pour utiliser l'accès à Lumio. Google fournit à SMART les données de compte nécessaires. Google SSO Protection des données de Google Google RGPD
Etats-Unis / Allemagne	Amazon Web Services, Inc.	Nécessaire pour le stockage. Nous proposons à la fois une option de stockage des données américaine et européenne. AWS Privacy (Foire aux questions sur la protection des données) AWS GPDR (Centre du Règlement général sur la protection des données (RGPD))

Utiliser Lumio en tant qu'élève connecté (contenus créés par les élèves)

Où	**Qui**	**Données et finalités**
Canada	SMART Technologies ULC	En option. En option. Lorsque les élèves participent à des activités en direct au cours desquelles ils donnent des réponses ou téléchargent des contenus qu'ils ont créés, ceux-ci sont associés à leur compte. SLS Terms (Conditions générales de vente SLS) RGPD - Décision d'adéquation de la CE Commission
Etats-Unis / Allemagne	Amazon Web Services, Inc.	Nécessaire pour le stockage. Nous proposons à la fois une option de stockage de données américaine et européenne. AWS Privacy (Foire aux questions sur la protection des données) AWS GPDR (Centre du Règlement général sur la protection des données (RGPD))
Etats-Unis / Belgique	Firebase (Google LLC)	Nécessaire pour la fonctionnalité de base (Firebase est une solution de cloud computing backend-as-a-service (BaaS) que nous utilisons pour le traitement informatique automatisé (temporaire) en temps réel). Firebase Privacy (protection des données et sécurité dans Firebase) Firebase RGPD (protection des données

Étudiant inscrit Analyse

Où	Qui	Données et finalités
Canada	SMART Technologies ULC	Nécessaire pour l'amélioration des produits et le suivi des services. Nous utilisons Mixpanel en tant que notre Sous-Traitant à ces fins. SLS Terms (Conditions générales de vente SLS) RGPD - Décision d'adéquation de la Commission européenne
Etats-Unis	Mixpanel Inc.	Nécessaire pour l'amélioration des produits et le suivi des services. Mixpanel nous permet d'analyser comment nos utilisateurs non identifiés interagissent avec Lumio. Il sert à identifier les tendances, à comprendre le comportement général agrégé des utilisateurs et nous aide à prendre de meilleures décisions sur la manière d'améliorer l'expérience utilisateur et les fonctionnalités de notre produit. Ces données sont également utilisées pour suivre le temps nécessaire à nos serveurs pour terminer des actions telles que l'ouverture de fichiers, ce qui nous aide à mesurer l'état du service et le temps de montée/descente. Mixpanel Privacy (Informations sur la protection des données) Mixpanel
K.A	Tiers	Contenu optionnel ou activités qu'un enseignant peut ajouter à une leçon, à partir de contenus tels que le contenu YouTube ou d'autres contenus intégrés qu'un utilisateur ajoute volontairement. Nous ne pouvons pas contrôler les données qu'un tiers transmet directement. Le contenu est collecté lorsqu'un enseignant ou un élève décide de l'inclure dans une leçon. Toutefois, dans le cas du contenu premium fourni par SMART, nous ne signalons que l'utilisation anonyme au fournisseur tiers.
Etats-Unis	Sentry.io	ID de la leçon (aucune donnée personnelle) ID d'utilisateur et ID de session (hachés et salés pour garantir l'anonymat) En-tête de la demande (application et version, plate-forme, système d'exploitation, navigateur, langue, date et heure) Breadcrumbs (dernières pages visitées et liens cliqués) Rapport d'erreur facultatif par l'utilisateur : une fois que le message d'erreur automatique est terminé, les utilisateurs ont la possibilité d'indiquer leur nom, leur adresse électronique et des informations supplémentaires sur l'erreur. Il est également demandé aux utilisateurs s'ils souhaitent que SMART les contacte. Ces informations personnelles facultatives sont

		stockées dans Salesforce (aux États-Unis) et transmises à notre équipe de service clientèle. Sentry Confidentialité Sentry
Etats-Unis	Slack Technologies LLC	• ID de la leçon (pas de données personnelles) • ID d'utilisateur et ID de session (hachés et salés pour préserver l'anonymat) • En-tête de la requête (application et version, plate-forme, système d'exploitation, navigateur, langue, date et heure) • Breadcrumbs (dernières pages visitées et liens cliqués) Rapport d'auto-échec facultatif : une fois que le rapport d'auto-échec automatique est terminée, les utilisateurs ont la possibilité d'indiquer leur nom, leur adresse électronique et des informations supplémentaires sur l'erreur. Il est également demandé aux utilisateurs s'ils souhaitent que SMART les contacte. Ces données personnelles facultatives sont stockées dans Salesforce (basé aux États-Unis) et partagées avec nos équipes d'assistance clientèle et de développement via Sentry et Slack. Confidentialité Slack Slack
Etats-Unis	Splunk Inc.	Métadonnées requises, y compris les journaux système et les performances. Confidentialité Splunk Splunk RGPD

ENSEIGNANTS/ADULTES, INSCRITS

Compte enseignant

Où	Qui	Données et finalités
Canada	SMART Technologies ULC	Détails du compte requis : nom d'affichage, nom, e-mail, adresse publique, numéro de téléphone, etc. Image de profil, préférence de

		langue. Paramètres requis du profil de compte : Opt-Ins, type d'utilisateur, localisation. SLS Terms (Conditions générales de vente SLS) RGPD - Décision d'adéquation de la CE Commission
Global	Microsoft, Inc.	Nécessaire si vous souhaitez utiliser Microsoft comme fournisseur d'authentification unique (SSO) pour utiliser l'accès à Lumio. Microsoft fournit à SMART les informations de compte nécessaires. Microsoft SSO Microsoft Privacy Microsoft RGPD
Global	Google LLC	Obligatoire si vous utilisez Google en tant que fournisseur d'authentification unique (SSO) pour utiliser l'accès à Lumio. Microsoft fournit à SMART les informations de compte nécessaires. Google SSO Confidentialité Google Google RGPD
Etats-Unis / Allemagne	Amazon Web Services, Inc.	Nécessaire pour le stockage. Nous proposons à la fois un site américaine ainsi qu'une option européenne de stockage des données. AWS Privacy (Foire aux questions sur la protection des données) AWS GPDR (Centre du Règlement général sur la protection des données (RGPD))

Utiliser Lumio en tant qu'enseignant connecté (contenus créés par les enseignants)

Où	**Qui**	**Données et finalités**
Canada	SMART Technologies ULC	Contenu généré (leçons créées par un enseignant et noms de classe choisis par l'utilisateur). SLS Terms (Conditions générales de vente SLS) RGPD - Décision d'adéquation de la CE Commission
Etats-Unis / Allemagne	Amazon Web Services, Inc.	Nécessaire pour le stockage. Nous proposons à la fois une option de stockage des données américaine et européenne. Protection des données AWS
Etats-Unis / Belgique	Firebase (Google LLC)	Nécessaire pour la fonctionnalité de base (Firebase est une solution de cloud computing backend-as-a-service (BaaS) que nous

		utilisons pour le traitement informatique automatisé (temporaire) en temps réel). Firebase Privacy (protection des données et sécurité dans Firebase) Firebase RGPD (protection des données

Enseignants inscrits Analytics

Où	Qui	Données et finalités
Canada	SMART Technologies ULC	Nécessaire pour l'amélioration des produits et le suivi des services. Nous utilisons Mixpanel comme notre Sous-Traitant à ces fins. SLS Terms (Conditions générales de vente SLS) RGPD - Décision d'adéquation de la CE Commission
Etats-Unis	Mixpanel, Inc	Nécessaire pour l'amélioration des produits et le suivi des services. Avec Mixpanel nous permet d'analyser comment nos utilisateurs non identifiés interagissent avec Lumio. Il sert à identifier les tendances, à comprendre le comportement général agrégé des utilisateurs et nous aide à prendre de meilleures décisions sur la manière d'améliorer l'expérience utilisateur et les fonctionnalités de notre produit. Ces données sont également utilisées pour suivre le temps nécessaire à nos serveurs pour terminer des actions telles que l'ouverture de fichiers, ce qui nous aide à mesurer l'état du service et le temps de montée/descente. Mixpanel Protection des données Mixpanel
K.A	Fournisseur tiers de contenu	Contenu ou activités facultatifs qu'un enseignant peut ajouter à une leçon, tels que le contenu YouTube ou tout autre contenu intégré qu'un utilisateur ajoute volontairement. Nous ne pouvons pas contrôler les données qu'un tiers collecte directement sur le contenu lorsqu'un enseignant ou un élève décide de l'inclure dans une leçon. Cependant, dans le cas du contenu premium fourni par SMART, nous ne signalons que l'utilisation anonyme au fournisseur tiers.
Etats-Unis	Sentry.io	• ID de la leçon (aucune donnée personnelle) • ID d'utilisateur et ID de session (hachés et salés pour garantir l'anonymat) • En-tête de la demande (application et version, plate-forme, système d'exploitation, navigateur, langue,

		date et heure) • Breadcrumbs (dernières pages visitées et liens cliqués) Rapport d'erreur facultatif par l'utilisateur : une fois que le message d'erreur automatique est terminé, les utilisateurs ont la possibilité d'indiquer leur nom, leur adresse électronique et des informations supplémentaires sur l'erreur. Il est également demandé aux utilisateurs s'ils souhaitent que SMART les contacte. Ces informations personnelles facultatives sont stockées dans Salesforce (aux États-Unis) et transmises à notre équipe de service clientèle.
Etats-Unis	Slack Technologies LLC	• ID de la leçon (pas de données personnelles) • ID d'utilisateur et ID de session (hachés et salés pour préserver l'anonymat) • En-tête de la requête (application et version, plate-forme, système d'exploitation, navigateur, langue, date et heure) Rapport d'auto-erreur facultatif : une fois que le rapport d'erreur automatique est terminé, les utilisateurs ont la possibilité d'indiquer leur nom, leur adresse électronique et des informations supplémentaires sur l'erreur. Il est également demandé aux utilisateurs s'ils souhaitent que SMART les contacte. Ces informations personnelles facultatives sont stockées dans Salesforce (basé aux États-Unis) et partagées avec nos équipes d'assistance clientèle et de développement via Sentry et Slack. Confidentialité Slack Slack RGPD
Etats-Unis	Splunk Inc.	Métadonnées requises, y compris les journaux système et les performances. Splunk Protection de la vie privée Splunk RGPD

DONNÉES CLIENTS COLLECTÉES ET TRAITÉES

Cette section décrit les données collectées, traitées et partagées avec les clients (acheteurs, prospects et distributeurs autorisés de SMART). Vous pouvez demander la suppression de vos données et de vos comptes à tout moment en contactant notre service clientèle, mais nous devons conserver toutes les données relatives aux achats et aux transactions financières jusqu'à ce qu'elles ne soient plus nécessaires conformément à la législation en vigueur. Le terme « identifiable » utilisé dans le tableau ci-dessous ne signifie pas nécessairement des données à caractère personnelle.

Où	Qui	Rôle	Données et finalités	Type
K.A.	Bureau régional de SMART	Revendeur / Vendeur	Requis : Informations de contact : nom de l'entreprise, e-mail, titre, téléphone, adresse. Nécessaire Informations sur la commande : Produit, quantité, prix et taxe, livraison. Renseignez-vous auprès de votre distributeur régional sur les informations sur la protection des données.	Identifiable
Canada	SMART Technologies ULC	Fabricant	Nécessaire Informations sur le compte : Nom de l'entreprise, e-mail, titre, téléphone, adresse, revendeurs, abonnements en cours. Informations requises pour la commande : Produit, quantité, prix et taxes, livraison. Informations requises sur le portail Admin pour le déploiement des licences : licences et activations, prénoms et noms des enseignants et des administrateurs (peut fournir une version de données non personnelles pour se conformer au RGPD) et adresses électroniques et noms de classe (peut fournir une version de données non personnelles pour se conformer au RGPD). SLS Terms (Conditions générales SLS) RGPD - EG Adequacy Decision (Décision d'adéquation de la Commission européenne)	Identifiable
Canada	Océan bleu Contact Centers, Inc.	Assistance	En option. Blue Ocean est un Sous-Traitant fournissant une assistance en direct (téléphone, e-mail et web). Les informations collectées comprennent le nom de l'entreprise, le nom de l'appelant (pour des raisons liées au RGPD, seul le nom de l'entreprise peut être utilisé), l'adresse électronique (pour des	Identifiable

			raisons liées au RGPD, une version ne contenant pas de données à caractère personnel peut également être fournie), le titre, le numéro de téléphone, l'adresse ainsi qu'une description du problème et tout détail commun permettant de résoudre le problème. Les appels sont enregistrés. Blue Ocean Protection des données RGPD - EG Adequacy Decision (décision d'adéquation de la européenne)	
États-Unis/Allemagne	Amazon Web Services, Inc.	Edition, back-office	Nécessaire pour l'infrastructure du produit, y compris l'hébergement des enregistrements des appels de support. Protection des données AWS AWS RGPD	Identifiable
Etats-Unis	Google, LLC	Edition, Office	Facultatif. Utilisé uniquement pour le traitement des formulaires d'assistance sont utilisés. Les formulaires Google sont utilisés lorsqu'un acheteur fait appel à notre service extérieur (par exemple, en cas d'assistance sur site). Google Google RGPD	Identifiable
Etats-Unis	Microsoft, Inc.	Edition, Office	Nécessaire pour notre système ERP (Enterprise Resource Planning), un logiciel qui gère les activités quotidiennes de l'entreprise telles que la comptabilité, l'approvisionnement, la gestion de projet et la chaîne d'approvisionnement, ainsi que pour notre système de messagerie électronique, PowerBI® (visite de données) et SharePoint® (gestion de documents), et pour tous les autres titres de logiciels Microsoft Office Protection des données Microsoft Microsoft RGPD	Identifiable

Etats-Unis	BigCommerce, Inc.	Commande	Facultatif. Utilisé uniquement lorsqu'un client fait un achat via notre boutique de commerce électronique : Nom du client, email, titre, téléphone, adresse, produit ou service acheté et si le paiement a été reçu. BigCommerce Protection des données BigCommerce RGPD	Identifiable
Etats-Unis	Stripe, Inc. et Stripe Payments Europe, Ltd.	Commande	Facultatif. Utilisé uniquement lorsqu'un client effectue un achat via notre boutique de commerce électronique avec une carte de crédit : Nom du client, e-mail, titre, téléphone, adresse, produit ou service acheté, données de la carte de crédit. Résidents de l'Espace économique européen (EEE), du Royaume-Uni et de la Suisse. Le responsable de la collecte et du traitement des données personnelles relatives aux cartes de crédit des résidents de l'EEE, du Royaume-Uni et de la Suisse est Stripe Payments Europe, Ltd, une société immatriculée en Irlande dont le siège social est situé 1 Grand Canal Street Lower, Grand Canal Dock, Dublin. Pour exercer vos droits, vous pouvez contacter le délégué à la protection des données à l'adresse dpo@stripe.com contacter. Stripe Stripe RGPD	Identifiable
Etats-Unis	Salesforce.com, Inc.	Commande, marketing, assistance à la vente	Nécessaire : informations sur les commandes, gestion de la relation client (CRM). Nécessaire pour que nos distributeurs et revendeurs agréés puissent travailler avec SMART peuvent être utilisés. Les informations de base sur les clients et les achats sont partagées entre SMART et ses distributeurs et revendeurs agréés. Salesforce Protection des données Commerciaux RGPD	Identifiable

Etats-Unis	HubSpot, Inc.	Marketing	Facultatif. Nous utilisons HubSpot, une gestion de la relation client (CRM), pour les personnes qui choisissent expressément ont choisi de recevoir certaines communications, par exemple des informations marketing, des formations, des nouvelles et des offres de notre part. Hubspot protection des données Hubspot RGPD	Identifiable
Etats-Unis	Mixpanel, Inc.	Surveillance	Nécessaire pour amélioration des produits et suivi des services. Mixpanel nous permet d'analyser la manière dont nos utilisateurs non identifiés interagissent avec Notebook. Il sert à identifier les tendances, comprendre le niveau général d'agrégation, le comportement d'utilisation et nous aide à prendre de meilleures décisions sur la façon d'améliorer la convivialité et les fonctionnalités de notre produit. Ces données sont également utilisées pour suivre la durée pendant laquelle nos serveurs ont besoin de terminer des actions telles que l'ouverture de fichiers, ce qui nous aide à mesurer l'état du service et le temps de montée/descente. Mixpanel Protection des données Mixpanel	Pseudonymisé
Etats-Unis	Gainsight, Inc.	Marketing	S'applique uniuqement aux clients situés aux Etats-Unis. Nous utilisons Gainsight, un outil de gestion de la relation client (CRM), pour le marketing par e-mail (nom, adresse e-mail, informations sur les entreprises) à des individus et à des organisations. Protection des données de Gainsight	Identifiable
Canada	CallMiner	Support	Facultatif . Traitement pour les interactions téléphoniques (option pour désactiver	Identifiable

			l'enregistrement des appels), requis pour les e-mails. Call Miner est un Sous-Traitant qui fournit des analyses d'interactions omnicanales basées sur l'IA et l'apprentissage automatique. Call Miner analyse les interactions de support client, y compris les appels et les e-mails enregistrés, qui sont temporairement stockés dans CallMiner. Les métadonnées sont stockées dans CallMiner afin d'analyser l'expérience client et de fournir des informations de tendance, et d'obtenir des interactions entre l'agent et le client. Confidentialité et sécurité de CallMiner Sécurité	
Etats-Unis ou Europe	Digital River		En option. Prise de commande en ligne (e-commerce). Utilisé uniquement lorsque des achats sont effectués via notre boutique de commerce électronique. SMART n'a pas accès aux informations relatives aux cartes de crédit, mais uniquement à Digital River. Confidentialité Digital River Digital River	Identifiable
Canada	Traitement de Fivetran Inc,	Backoffice	Service de connecteurs de données requis. Déplace les données des applications système vers Snowflake. Fivetran Protection de la vie privée Fivetran Sécurité	Informations identifiables sur le compte et les achats
Royaume-Uni	Kluster Enterprises Limited	Prévision des ventes	Nécessaire pour effectuer des analyses de nos données de vente. Kluster Privacy Kluster	Informations identifiables sur le compte et les achats
Etats-Unis	LinkedIn	Marketing	Obligatoire si vous choisissez de recevoir des communications marketing. Utilisé pour créer une audience de proximité susceptible d'être intéressée par SMART parce qu'elle ressemble à des personnes qui ont déjà explicitement demandé à participer à la campagne et demandé à recevoir certaines	Informations identifiables sur le compte et les achats

			communications, telles que le marketing, les solutions SMART, les événements et les offres spéciales. Confidentialité LinkedIn LinkedIn RGPD	
Etats-Unis	Meta Platforms, Inc.	Marketing	Nécessaire si vous souhaitez choisissent de recevoir des communications marketing. Utilisé pour créer une audience ciblée susceptible d'être intéressée par SMART parce qu'elle ressemble à des personnes qui ont déjà expressément choisi de recevoir certaines communications, comme le marketing, les solutions SMART, les événements et les offres spéciales. Meta Platforms	Informations de contact identifiables
Etats-Unis	Outreach Corporation	Marketing	Obligatoire si vous choisissez de recevoir des communications marketing. Outreach est utilisé pour contacter nos clients en Amérique du Nord qui ont expressément choisi de recevoir certaines communications telles que le marketing, les formations, les actualités et les offres de notre part. Outreach propose des analyses. Outreach Privacy Sécurité de proximité	Informations identifiables sur le compte et les achats.
Canada	Sana Commerce	Ordre	Nécessaire uniquement si le Client identifiable achète des pièces. Traiter le compte et vous commandez et informations sur les achats Paiements (en cas d'utilisation de Sana Pay). Sana Privacy	Traiter les informations sur les achats.
Etats-Unis	Sigma Computing, Inc.	Traitement, back office	Nécessaire pour les applications web qui présentent des données Snowflake (voir ci-dessous) aux utilisateurs internes. Sigma	Informations identifiables sur le compte et les achats
Canada	Snowflake, Inc.	Traitement, back office	Nécessaire. Snowflake agrège et centralise les données clients de SMART provenant de plusieurs sources (Salesforce, Microsoft Dynamics, HubSpot,	Informations identifiables sur le compte et les achats

			Oracle/OBIEE, Pivotal). Requis pour le traitement et le back-office. Protection de la vie privée Snowflake Sécurité Snowflake	