

CONVENTION DE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL (DPA) ProECO 4 / ProPMS

Introduction

Scolares, en tant que sous-traitant au sens du Règlement général sur la protection des données (RGPD) et ses clients (école ou pouvoir organisateur) en tant que Responsable de Traitement conviennent que le présent document sur la protection des données des produits et services ("DPA") définit leurs obligations en matière de traitement et de sécurité des données des clients, des données des services professionnels et des données personnelles dans le cadre des produits et services. Ce DPA fait partie intégrante du contrat entre le Responsable de Traitement est Scolares. Ce DPA peut être amené à évoluer, en fonction des services proposés par le Responsable de Traitement ou en vertu de l'évolution de la législation concernant la protection des données personnelles. Les évolutions de ce DPA seront communiquées au Responsable de Traitement par courriel et la version adaptée sera publiée sur le site de Scolares avec la date d'entrée en vigueur.

Article 1 : Définitions

Les termes suivants, commençant par une majuscule, utilisés dans le présent DPA ont, sauf indication claire ressortant du contexte, le sens qui leur est donné dans le présent article :

- a) « Relation Contractuelle » le contrat principal conclu entre les Parties définissant la livraison des services et/ou des produits ou la collaboration entre eux, y compris toutes ses modifications et annexes et tout ce qui est convenu ultérieurement entre les Parties au sujet du présent DPA ;
- b) Réglementation Applicable en matière de « Protection des Données » : toutes les réglementations relatives à la protection des données qui sont applicables au Traitement et à l'utilisation des Données à Caractère Personnel dans le contexte des activités menées dans le cadre de la Relation Contractuelle, y compris le Règlement général sur la protection des données (comme défini ci-après) ;
- c) « DPA » la présente convention de traitement des données à caractère personnel, y compris ses annexes ;
- d) « RGPD » le règlement général sur la protection des données (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 applicable à compter du 25 mai 2018 ;
- e) « Données à Caractère Personnel » selon la définition du RGPD
- f) « Traiter » ou « Traitement » selon la définition du RGPD ;
- g) « Violation de Données à Caractère personnel » selon la définition du RGPD ;

- h) « Mesures Techniques et Organisationnelles » les mesures techniques et organisationnelles telles que définies dans le RGPD et mises en place par le Responsable du Traitement et le Sous-traitant ;
- i) « Autorité de contrôle » une autorité publique indépendante instituée par un État membre de l'Union européenne en exécution de l'article 51 du RGPD, en Belgique, l'autorité de protection des données ;
- j) « Collaborateur » : toute personne travaillant pour le sous-traitant, qu'elle soit employée, stagiaire, intérimaire étudiante ou consultante ;
- k) Sous-traitant Ultérieur : ce sont les sous-traitant de Scolares définie dans l'annexe 3 ;
- l) Scolares : fournisseur de logiciel et de solutions informatique, sous-traitant au sens du RGPD ;
- m) Client : Ecole ou pouvoir organisateur (PO) : client de Scolares et Responsable de Traitement au sens du RGPD ;
- n) Parties : Scolares et son Client.

Article 2 : Objet du DPA

- a) Le présent DPA a pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à effectuer pour le compte du Responsable du Traitement les opérations de Traitement de Données à Caractère Personnel définies dans la Relation Contractuelle et/ou décrites en annexe 1 du présent DPA. Dans le cadre de leur Relation Contractuelle, les Parties s'engagent à respecter la Réglementation en vigueur applicable aux Traitements de Données à Caractère Personnel et, en particulier, le RGPD.
- b) En cas de conflit entre les différents contrats régissant la Relation Contractuelle et le Présent DPA, les dispositions du présent DPA prévaudront.

Article 3 : Durée de la convention

- a) Le présent DPA entre en vigueur à compter de la date d'entrée en vigueur de la Relation Contractuelle.
- b) Le Sous-traitant peut Traiter les Données à Caractère Personnel transmises par le Responsable du Traitement aussi longtemps que nécessaire pour l'exécution de la mission telle que spécifiée dans la Relation Contractuelle ou dans l'annexe 1 du présent DPA.

Article 4 : Obligations du Sous-traitant

Le Sous-traitant s'engage à respecter les obligations suivantes :

Article 4.1 : Traitement des Données :

1. Le Sous-traitant s'engage à Traiter les Données conformément aux instructions écrites du Responsable du Traitement contenues dans la Relation Contractuelle et/ou décrites dans l'annexe 1 du présent DPA.
2. Si le Sous-traitant considère raisonnablement qu'une instruction constitue une violation du RGPD ou d'autres dispositions du droit de l'Union européenne ou du droit des états membres relatives à la Protection des Données (« Instruction Contestée »), il en informe immédiatement le Responsable du Traitement.
3. En cas d'une telle notification, le Sous-traitant est autorisé (1) à suspendre l'exécution de ladite Instruction Contestée et (2) de continuer à Traiter les Données à Caractère Personnel conformément aux instructions reçues précédemment et/ou prévues par la Relation Contractuelle et dans l'annexe 1. Le Responsable du Traitement n'aura pas droit, pour cela, à une indemnisation ou dédommagement.

Article 4.2 : Confidentialité :

1. Le Sous-traitant s'engage à garantir la confidentialité des Données à Caractère Personnel Traitées dans le cadre de la Relation Contractuelle entre les Parties. À cette fin, l'accès aux Données à Caractère Personnel est strictement limité par le Sous-traitant aux personnes qui, dans le cadre de l'exécution de Relation Contractuelle entre les Parties, doivent y avoir accès ou en avoir connaissance. L'obligation de confidentialité reste en vigueur après la cessation de la Relation Contractuelle entre les Parties.
2. La clause de confidentialité signée par tous les collaborateurs travaillant pour le sous-traitant est jointe en annexe 4.
3. Le Sous-traitant veille à ce que toutes les personnes concernées dans le Traitement des Données à caractère personnel, y compris ses collaborateurs, représentants et/ou Sous-traitants, traitent ces données de manière confidentielle.
4. Le Sous-traitant s'engage à ce que ses collaborateurs n'aient accès aux Données à Caractère Personnel que dans la mesure nécessaire à l'exécution de leur travail, s'engagent à respecter la confidentialité et soient sensibilisées en matière de protection des Données à Caractère Personnel.
5. Ces accès aux données et communications de données et toutes conséquences de ceux-ci se font sous la seule et entière responsabilité du Responsable de Traitement qui peut démontrer avoir la base légale nécessaire pour ces accès, traitements et communications de données.

Article 4.3 : Mesures Techniques et Organisationnelles :

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du Traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le Sous-traitant met en œuvre les Mesures Techniques et Organisationnelles appropriées afin de garantir un niveau de sécurité adaptés au risque.
2. Ces Mesures Techniques et Organisationnelles reprendront, inter alia et le cas échéant, la liste des mesures de sécurité minimales applicables reprise en annexe 2 du présent DPA, que le Responsable évalue comme étant suffisantes et appropriées.
3. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le Traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de Données à Caractère Personnel transmises, conservées ou Traitées d'une autre manière, ou de l'accès non autorisé à de telles Données, de manière accidentelle ou illicite.

Article 4.5: Sous-traitance Ultérieure

1. Le Sous-traitant est autorisé à faire appel à un autre Sous-traitant (ci-après le Sous-traitant Ultérieur). Par la signature du présent DPA, le Responsable de Traitement accorde au Sous-traitant l'autorisation générale de recruter des Sous-traitants Ultérieurs.

Le Sous-traitant peut continuer à travailler avec les Sous-traitants Ultérieurs qui avaient déjà été désignés à la date de prise d'effet du DPA (voir annexe 3), à condition de répondre dans les plus brefs délais aux conditions suivantes qui s'appliquent à toute Sous-traitance ultérieure :

- a) Le Sous-traitant doit s'assurer au préalable que le Sous-traitant Ultérieur présente des garanties suffisantes quant à la mise en œuvre de Mesures Techniques et Organisationnelles appropriées de manière que le Traitement réponde aux exigences du RGPD.
 - b) Le Sous-traitant impose contractuellement au Sous-traitant Ultérieur des obligations équivalentes en matière de protection des Données que celles fixées dans l'article 4 du présent DPA.
2. L'autorisation générale de recours à des sous-traitance ultérieurs, ne concerne pas l'engagement de personnel temporairement par le Sous-Traitant pour remplacer un collaborateur absent ou pour étoffer l'équipe en cas de besoins, et pour lesquels le Responsable de Traitement accorde au Sous-traitant une autorisation générale et systématique sans nécessité d'information.

3. Le Sous-traitant s'engage à informer par écrit (électronique ou papier) le Responsable de Traitement des changements envisagés au sujet de l'ajout d'un nouveau Sous-traitant Ulérieur ou du remplacement d'un Sous-traitant Ulérieur existant. Le Responsable de Traitement dispose d'un délai de quatorze (14) jours à compter du jour de la réception de cette information pour émettre ses objections documentées par rapport à la capacité du Sous-traitant de protéger des Données à caractère Personnel et d'en garantir la confidentialité. Cette sous-traitance ne peut être effectuée que si le Responsable de Traitement n'a pas émis d'objection pendant le délai convenu de 14 jours.
4. Si le Sous-traitant Ulérieur ne remplit pas ses obligations en matière de Protection des données, le Sous-traitant demeure pleinement responsable devant le Responsable du Traitement de l'exécution par le Sous-traitant Ulérieur de ses obligations.

Article 4.6: Droits des Personnes Concernées

1. Il appartient au Responsable du Traitement de fournir aux personnes concernées les informations prévues ainsi que de respecter toutes les obligations relatives à leurs droits (chapitre III du RGPD).
2. Dans la mesure du possible, en tenant compte de la nature du Traitement, et au moyen de Mesures Techniques et Organisationnelles appropriées, le Sous-traitant fournira toute l'aide raisonnable pour permettre au Responsable du Traitement de remplir son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.
3. Les Parties ne se facturent pas l'une à l'autre l'assistance raisonnable fournie. Si compte tenu de la complexité de la demande, l'une des Parties souhaite facturer des frais, elle en informe préalablement l'autre Partie dans un délai raisonnable.

Article 4.7 : Aide au Responsable de Traitement en matière d'analyse d'impact et de consultation préalable

1. Le Sous-traitant aide le Responsable du Traitement à garantir le respect des obligations qui lui incombent en matière d'analyse d'impact et de consultation préalable (articles 35 à 36 du RGPD), compte tenu de la nature du Traitement et des informations à la disposition du Sous-traitant (sauf si l'information utile à ces fins est déjà à la disposition du Responsable du Traitement).
2. Cette assistance sera facturée par le Sous-traitant au Responsable, à titre de rémunération supplémentaire, sur la base d'un devis.

Article 4.8 : Violation de Données à Caractère Personnel

1. Si une Partie détecte une Violation de Données à Caractère Personnel, elle en informera l'autre Partie sans délai déraisonnable dès qu'elle aura connaissance de la Violation de Données à Caractère Personnel, que cette Violation de Données à Caractère Personnel soit ou ne soit pas susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques visés à l'article 34, paragraphe 1, du RGPD. Cette information sera accompagnée, dans la mesure du possible, de toute documentation utile afin de permettre aux Parties, si nécessaire, de notifier cette Violation à l'Autorité de contrôle compétente.
2. En cas de Violation des Données, le Responsable de Traitement se conforme à toute obligation légale de déclaration auprès de l'Autorité de protection des données et de communication aux personnes concernées.
3. Les Parties conviennent de bonne foi, dans le cadre d'une consultation mutuelle, de la répartition raisonnable des coûts liés au respect des obligations de déclaration.
4. Dans le cas où une Violation de Données chez le Sous-traitant affecte plusieurs Responsables de traitement de manière égale, le Sous-traitant peut, après consultation d'un ou plusieurs Responsables du Traitement, signaler la Violation de Données à l'Autorité de protection des Données au nom des Responsables de traitement. Le Sous-traitant informera immédiatement le Responsable de Traitement (et si possible avant la notification) de son intention de le faire.
5. Dans le cas où la Violation des Données chez le Sous-traitant est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, le Responsable de Traitement informera les personnes concernées de la Violation des Données à Caractère Personnel.
6. Les Parties documentent toutes les Violations de Données à Caractère Personnel dans un registre (d'incidents), y compris les faits concernant la Violation de Données à Caractère Personnel, ses conséquences et les mesures correctives prises.
7. Le Sous-traitant informera le Responsable de Traitement, conformément aux accords prévus à l'annexe 2, des incidents de sécurité, autres qu'une Violation de Données à Caractère Personnel, qui ne relèvent pas du champ d'application de l'article 1 paragraphe f du présent DPA.

Article 4.9 : Suppression ou restitution des Données à Caractère Personnel

1. Le Sous-traitant supprimera ou fera supprimer (en ce compris par les Sous-traitants Ultérieurs) toutes les copies des Données à Caractère Personnel du Responsable du Traitement, dans les meilleurs délais et, en tout cas, dans les 30 jours à compter de la

date à laquelle la prestation de service relative au Traitement des Données à Caractère Personnel a pris fin (Date de fin).

2. Si en vertu du droit de l'Union européenne ou du droit de l'état membre, le Sous-Traitant est tenu de conserver, pour une période imposée, les Données à Caractère Personnel du Responsable du Traitement, les délais indiqués ci-dessus ne commenceront à courir qu'à la fin de la période imposée. Dans ce cas, le Sous-traitant garantira la confidentialité de ces Données à Caractère Personnel et veillera à ce que ces Données à Caractère Personnel du Responsable du Traitement soient Traitées exclusivement aux fins spécifiées dans les législations qui imposent de les conserver.

Article 4.10 : Documentation et droits d'audit

1. À la demande du Responsable du Traitement, le Sous-traitant mettra à disposition toutes les informations nécessaires afin de démontrer le respect du présent DPA, et pour permettre la réalisation d'audit ou d'inspections par le Responsable du Traitement lui-même ou par un auditeur qu'il a mandaté à cet effet.
2. Lorsque ces informations ne sont pas confidentielles ou sensibles, elles seront rendues accessibles par le Sous-traitant par le biais d'un processus simple (par exemple, via le site Web du Responsable). Lorsque les informations sont confidentielles, le Sous-traitant peut les mettre à la disposition du Responsable sur demande, mais peut exiger du Responsable qu'il signe d'abord une convention de non-divulgaration proposée par le Sous-Traitant. Le Sous-traitant peut néanmoins, à sa seule discrétion, choisir de ne pas divulguer certaines informations de sécurité hautement sensibles, telle que le contenu intégral d'une DPIA.
3. Le Sous-traitant peut exiger que le Responsable paie les frais pour ces informations (les frais supplémentaires seront basés sur un devis et ne seront pas utilisés pour empêcher le Responsable d'accéder aux renseignements sur les contrôles de sécurité du service).
4. Si, de l'avis raisonnable du Responsable, des renseignements suffisants pour confirmer et démontrer la conformité aux modalités du présent DPA ne sont pas fournis, le Responsable a le droit de nommer un tiers vérificateur indépendant possédant les qualifications professionnelles requises et lié par une obligation de confidentialité, lequel vérificateur doit être accepté par le Sous-traitant, pour vérifier sa conformité du présent DPA et aux lois de protection des données requises pour déterminer si les déclarations soumises par le Sous-traitant en vertu du présente DPA sont véridiques et complètes. Le refus d'un vérificateur par le Sous-Traitant doit être dument motivé. Le Sous-traitant a notamment le droit de s'opposer à la désignation

d'un auditeur dans le chef duquel il pourrait exister un conflit d'intérêt ou un risque en termes de protection des secrets d'affaires ou de la confidentialité.

5. Le Responsable et le Sous-traitant doivent s'entendre sur l'étendue, le moment et la durée de la vérification. Le Responsable doit aviser sans délai le Sous-traitant de toute non-conformité constatée au cours d'un audit. Le Responsable ne peut pas auditer le Sous-traitant plus d'une fois par an. Le Responsable est responsable de tous les coûts et honoraires liés à une telle vérification, y compris, mais sans s'y limiter, les honoraires professionnels de tout vérificateur et tous les coûts et honoraires raisonnables pour le temps que le Sous-traitant consacre à une telle vérification, lesquels seront facturés par le Sous-traitant à titre de rémunération horaire supplémentaire. Toutes les informations traitées ou créées au cours d'un audit seront considérées comme étant des informations confidentielles du Sous-traitant, et le rapport d'audit sera fourni au Sous-traitant. Avant de partager ces informations avec le Responsable, ce dernier peut exiger que le Responsable qu'il signe d'abord un accord de non-divulgence que le Sous-traitant juge acceptable.
6. Toute demande d'audit devra être formulée par écrit au minimum 15 jours ouvrables à l'avance par le Responsable du Traitement. L'audit n'aura lieu que pendant les heures de travail et sans perturber substantiellement les activités opérationnelles du Sous-traitant.
7. Si une Autorité de contrôle exige un audit afin de vérifier ou de contrôler le respect par le Responsable des lois sur la protection des données, le Sous-traitant coopérera à cet audit. De même, les coûts d'un tel audit sont à la charge du Responsable.

Article 5 : Responsabilité

Afin de lever toute ambiguïté, il est souligné que le Sous-traitant ne sera pas responsable envers le Responsable du Traitement d'une infraction quelconque à la Règlementation Applicable en matière de Protection des Données imputable en tout ou en partie au Responsable du Traitement ou ses instructions.

Les dispositions du présent article sont sans préjudice des voies de recours dont dispose la Partie accusée en vertu des lois ou règlements applicables.

Article 6 : Dispositions finales

Article 6.1 : Compétence et droit applicable

Les Parties déclarent que la juridiction compétente (unique ou exclusive) déterminée dans la Relation Contractuelle entre les Parties sera également compétente pour tout litige et toutes prétentions qui naîtraient du fait de ce DPA, en ce compris les litiges éventuels à propos de

son existence, de sa validité en droit ou de sa résiliation ou encore des conséquences de sa nullité.

Les Parties déclarent que ce DPA, de même que toutes les obligations non contractuelles ou autres attachées à ce DPA, seront régies par la loi belge.

Article 6.2 : Validité et caractère exécutoire

L'invalidité ou le caractère non exécutoire d'une disposition du DPA, quelle qu'elle soit, n'a aucune influence sur la validité ou le caractère exécutoire des autres dispositions du DPA. La disposition correspondante sera, soit (1) remplacée par une disposition valable et exécutoire qui se rapproche le plus de l'intention initiale des Parties.

Annexe 1 : Détails du traitement des données à caractère personnel du Responsable de Traitement

Annexe 2 : Mesures de sécurité minimales applicables

Annexe 3 : Liste des sous-traitants ultérieurs

Annexe 4 : Clause de confidentialité

Annexe 1 : DÉTAILS DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU RESPONSABLE DE TRAITEMENT

La présente Annexe 1 contient certaines précisions à propos du Traitement des Données à Caractère Personnel du Responsable du Traitement, telles qu'elles sont stipulées par l'article 28(3) du RGPD.

A. Objet et durée du Traitement des Données à Caractère Personnel du Responsable du Traitement

L'objet et la durée du Traitement des Données à Caractère Personnel du Responsable du Traitement sont décrits dans la Relation Contractuelle et la présente annexe.

- a. Traitement de données à caractère personnel du Client, dans le cadre de la fourniture à ce dernier des différents produits/services informatiques du Sous-traitant tels que, notamment, licence de logiciel, hébergement, application en ligne (SaaS), installation, support technique ou fonctionnel, intégration avec des solutions tierces, formations pendant la durée de la licence, de la fourniture ou de l'intervention.
- b. Traitement de données à caractère personnel du client Responsable du Traitement, par le Sous-traitant, pendant la durée des tests internes à mener dans le cadre de la maintenance et du développement des différents produits/services informatiques du Sous-traitant.

La durée des traitements est liée à la relation contractuelle et les Traitements de Données se termineront conformément aux conditions de clôture des relations contractuelles.

B. La nature et l'objet (finalité) du Traitement des Données à Caractère Personnel du Responsable du Traitement

- a. Accès à, et le cas échéant intervention ponctuelle sur, des bases de données client (ou copie de celles-ci), dans le cadre de l'assistance ou du support technique, à la demande et/ou avec l'accord du client.
- b. Installation, récupération, fusion et autres opérations sur bases de données client, à la demande et/ou avec l'accord du client.
- c. Stockage et sauvegarde de bases de données client, en cas d'hébergement ou de fourniture d'une application en ligne.

- d. Transfert et synchronisation de données administratives en vue d'alimenter différentes applications, à la demande et/ou avec l'accord du client.
- e. Intégration avec des solutions tierces, à la demande et/ou avec l'accord du client. Utilisation des données du client lors d'une formation qui lui est réservée, à la demande du client.
- f. Accès aux bases de données client, ainsi que copie, récupération, stockage, sauvegarde, installation, utilisation de celles-ci et tout autre traitement nécessaire dans le cadre et pour les besoins des tests internes à réaliser conformément à l'autorisation donnée par le Responsable du Traitement.

C. Les types de Données à Caractère Personnel du Responsable du Traitement

- a. Données administratives d'identification personnelles ;
- b. Données administratives d'identification financières ;
- c. D'une manière générale toutes données à caractère personnel collectées par le client, Responsable du Traitement, susceptibles d'être traitées par les logiciels, applications et services fournis par le Sous-traitant.

D. Les catégories de personnes concernées auxquelles se rapportent les Données à Caractère Personnel du Responsable du Traitement

a. ProEco 4

- o Elèves ;
- o Enseignants ;
- o Membres du personnel du Responsable de Traitement ;
- o Parents et Responsables légaux ;
- o Utilisateurs et membres du Pouvoir Organisateur.

b. ProPMS

- o Elèves ;
- o Membres du personnel du Responsable de Traitement ;
- o Parents et Responsables légaux ;
- o Utilisateurs et membres du Pouvoir Organisateur.

E. Les destinataires des Données à Caractère Personnel autorisés par le Responsable de Traitement à la date de conclusion du DPA:

Par la présente le Responsable du Traitement, ayant souscrit un contrat concernant l'utilisation de ProEco 4, autorise expressément le Sous-traitant à donner accès et communiquer tout ou partie des données :

- a. À la Fédération Wallonie- Bruxelles en vertu des obligations légales qui s'imposent au Responsable de Traitement ;
- b. Au SeGEC en vertu de l'accord signé entre le Responsable de Traitement et le SeGEC ;
- c. Au centre PMS lié structurellement au Responsable du traitement et uniquement à celui-ci, et ce en vertu des relations contractuelles entre le Responsable du Traitement et ce centre PMS ;
- d. A l'Office National de la Sécurité Sociale : en application de la disposition légale imposant aux établissements scolaires la mise en œuvre d'une DIMONA pour l'ensemble des stages ;
- e. À la plateforme « Questi » en vertu du contrat signé entre le Responsable de Traitement et cette plateforme
- f. À la plateforme « Itslearning » en vertu du contrat signé entre le Responsable de Traitement et cette plateforme ;
- g. À plateforme « Portima » en vertu du contrat signé entre le Responsable de Traitement et la plateforme ;
- h. À la plateforme « Résultats Epreuves » en vertu de l'accord signé entre Le Responsable De Traitement et le SeGEC ;
- i. Au logiciel ComptEco en vertu du contrat signé entre le Responsable de Traitement et Scolares ;
- j. Au Logiciel Anciennetés en vertu du contrat signé entre le Responsable de Traitement et Scolares ;
- k. Au logiciel Bob en vertu du contrat signé entre le Responsable de Traitement et le fournisseur de l'application ;
- l. Au logiciel EDT en vertu du contrat signé entre le Responsable de Traitement et Scolares.

Le Responsable de Traitement, ayant souscrit un contrat pour l'utilisation du logiciel ProPMS, autorise expressément le Sous-traitant à donner accès et communiquer tout ou partie des données : :

- a. Au Logiciel Anciennetés en vertu du contrat signé entre le Responsable de Traitement et Scolares.

Annexe 2 : MESURES DE SECURITE MINIMALES APPLICABLES

A. Politique de sécurité

- a) Le Sous-traitant dispose de procédures de sécurité, qui sont revues et adaptées périodiquement.
- b) Les mesures de sécurité sont communiquées au personnel autorisé et leur application est contrôlée.

B. Organisation de la sécurité

- a) Les responsabilités en matière de sécurité sont définies et attribuées chez le Sous-traitant.
- b) Un DPO externe a été désigné chez le Sous-traitant.

C. Ressources Humaines

- a) Les collaborateurs internes et externes du Sous-traitant sont sensibilisés à la sécurité de l'information et des données à caractère personnel en particulier.
- b) Des clauses de confidentialité ont été signées par les membres du personnel

D. Gestion des actifs

- a) Le Sous-traitant dispose d'un inventaire des actifs régulièrement mis à jour.
- b) Les règles d'utilisation de ces actifs sont définies et clairement communiquées.

E. Sécurité physique et environnementale

- a) Les locaux du Sous-traitant où se trouvent les informations, les données ainsi que leurs dispositifs de traitement disposent d'un accès sécurisé.

F. Sécurité Opérationnelle

- a) Le Sous-traitant met en place des mesures anti-virus et anti-malware afin de prévenir toute altération ou vols de données à l'aide de logiciels malveillants.
- b) Ces protections et ces logiciels sont régulièrement mises à jour.
- c) Le Sous-traitant dispose d'un processus de gestion des accès.
- d) L'accès des collaborateurs est limité aux informations nécessaires à l'exercice de leur fonction.
- e) Les droits d'administrateur sur les systèmes sont strictement limités aux personnes indispensables.
- f) Le Sous-traitant dispose d'une politique en matière de mot de passe (incl. Caractères spéciaux, longueur minimum, changement régulier).

- g) Le Sous-traitant a mis en place une politique de Backup, avec un temps de rétention limité, qui permet la restauration des données en cas de besoin (perte, dommage, vol,).
- h) Des tests de restauration sont régulièrement effectués.
- i) L'utilisation des médias de stockage (USB, disque dur externe, ...) est réglementée.
- j) Aucune donnée ne peut être sauvegardée sur un média n'appartenant pas au Sous-traitant.

G. Sécurité des communications

- a) Le Sous-traitant utilise des mesures de sécurité pour protéger les transferts d'informations en utilisant des protocoles sécurisés.

H. Développement et maintenance d'applications ou de systèmes

- a) Le Sous-traitant veille à ce que les exigences de sécurité soient garanties lors du développement et la maintenance de logiciels et de systèmes.
- b) Le « privacy by design » et « by default » est mis en place pour les nouveaux projets
- c) Les analyses de risques (DPIA) sont effectuées en conformité avec le RGPD.
- d) Les procédures liées au « change management » sont documentées (point de contrôle et validation)
- e) Le Sous-traitant sépare les environnements de développement et de test de l'environnement de production.
- f) Le Sous-traitant veille à la sécurité des systèmes et à effectuer des tests avant utilisation.

I. Gestion des incidents

- a) Le Sous-traitant dispose d'une procédure de gestion des incidents documentée et communiquée au personnel et aux tiers autorisés.
- b) L'avis du DPO est sollicité pour chaque incident
- c) Tous les incidents et les mesures correctives sont documentés
- d) La communication au Responsable de Traitement est organisée de façon à prévenir celui-ci conformément aux relations contractuelles et au RGPD

J. Continuité

- a) Le Sous-traitant limite les risques de panne des systèmes par une bonne maintenance et dans certains cas par une redondance.
- b) Un plan de restauration des systèmes est établi par le Sous-traitant et / ou ses sous-traitant ultérieurs.
- c) Des mécanismes de restauration sont mis en place et le personnel est sensibilisé.

Annexe 3 : LISTE DES SOUS-TRAITANTS ULTÉRIEURS

<i>Nom du Sous-traitant</i>	<i>Localisation</i>	<i>Activité de traitement</i>
Microsoft Azure	UE	Hébergement des serveurs de Scolares
CM Telecom	UE	Passerelle d'envoi SMS
Allocloud	UE	Service de téléphonie par VoIP dans le « cloud ».
Zoho Desk	USA	Customer service (plateforme ticket support)
Sendgrid	UE (BE)	Passerelle d'envoi de mails
WaveNet	UE (BE)	Développement
Abelaro	UE (BE)	Développement
All4IS	UE (BE)	Développement
Degetel	UE (BE)	Gestion de l'infrastructure

Annexe 4 : CLAUSE DE CONFIDENTIALITÉ

- A. Pour permettre au « Collaborateur » de mener à bien le travail qui lui est demandé, « Scolares » est amené à communiquer au « Collaborateur » des données personnelles de tiers (clients, témoins, prospects, etc.) soit verbalement, soit sous forme de documents écrits ou électroniques.
- B. L'utilisation de ces données personnelles est soumise à une réglementation stricte et notamment le règlement européen de protection des données personnelles (RGPD) pour lequel « Scolares » a mis en place les mesures de sécurité techniques et organisationnelles appropriées. Le respect strict de la confidentialité des données personnelles gérées par « Scolares » fait partie intégrante de ces mesures et fait l'objet du présent avenant.
- C. « Scolares » ne donnera accès à ces données personnelles que si le « détaché » en a besoin dans l'exercice de son activité professionnelle.
- D. Ces informations sont communiquées au Collaborateur, à charge pour lui de respecter les engagements suivants :
- E. Garder strictement confidentielles, ne pas publier, ne pas divulguer à des tiers, les données personnelles de quelque nature qu'elles soient qui lui auront été communiquées par « Scolares », qu'elles appartiennent à « Scolares » ou à une tierce personne, ou auxquelles il aurait accès ou qui seraient le résultat de ses propres prestations,
- F. Ne pas utiliser ces données personnelles, directement ou indirectement, pour ses propres besoins autres que la réalisation de la prestation qui lui est demandée.
- G. Ne communiquer ces données personnelles qu'en fonction des instructions de « Scolares », uniquement à ceux qui auraient besoin de les connaître pour réaliser leurs prestations.
- H. Ne communiquer ces données à aucun tiers sans instruction du « Scolares ».
- I. Ne pas dupliquer les documents (de quelque nature qu'ils soient), remis par « Scolares » pour en faire un usage personnel ou en dehors des instructions du « Scolares »
- J. Respecter scrupuleusement les mesures techniques et organisationnelles mises en place par « Scolares » concernant la protection des données personnelles.
- K. Informer immédiatement « Scolares » si le « Collaborateur » a connaissance d'une divulgation, d'une tentative de divulgation de données personnelles. Dans ce cadre, le « Collaborateur » prendra toutes les mesures nécessaires à son niveau pour sauvegarder les intérêts de « Scolares ».
- L. Tenant compte de la pérennité de la confidentialité, le présent accord de confidentialité prendra ses effets dès le premier jour de la mission confiée au « Collaborateur » et restera d'application durant les 24 mois qui suivent la fin des relations contractuelles entre « Scolares » et le « Collaborateur ».

- M. Le présent Accord est régi par le droit belge.
- N. Tout litige portant sur l'exécution ou l'interprétation du présent Accord devra faire l'objet d'une conciliation préalable entre les parties. Si un règlement s'avère impossible, le litige sera soumis aux juridictions de l'arrondissement de Bruxelles siégeant en langue française.