ANNEXE 2. Mesures de sécurité techniques et organisationnelles générales

Conformément à l'article 28.1 du RGPD, le responsable du traitement fait exclusivement appel à des sous-traitants présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles, afin de garantir la protection adéquate des données à caractère personnel et des droits des personnes concernées.

Conformément à l'article 32 du RGPD, le sous-traitant est tenu de prendre des mesures techniques et organisationnelles appropriées pour sécuriser le traitement des données à caractère personnel.

Dans la présente annexe, les sous-traitants énumèrent les mesures de sécurité techniques et organisationnelles générales qu'ils ont prises afin d'apporter des garanties suffisantes au responsable du traitement quant à la protection des données à caractère personnel.

Certifications éventuelles :

Audits / déclarations de tiers :

Description générale des mesures visées à l'article 7.2 du contrat de sous-traitance

I. Description générale des mesures destinées à garantir que seul le personnel autorisé a accès au traitement des données à caractère personnel

Plus précisément, la manière dont sont défini(e)s les (catégories de) collaborateurs du sous-traitant qui ont accès à tel ou tel type de données à caractère personnel, y compris une description des actes que ces collaborateurs sont autorisés à accomplir avec les données à caractère personnel

Plantyn applique une politique d'autorisation pour déterminer qui doit avoir accès à telles ou telles données. Cette catégorisation permet de s'assurer que les collaborateurs n'ont pas accès à plus de données que strictement nécessaire dans le cadre de leur fonction.

Collaborateurs et données	Actes
Les collaborateurs du service clientèle et les consultants ont accès, sur demande d'une école, aux informations relatives aux licences. Ils peuvent voir, entre autres, quels élèves ont activé tel ou tel outil d'apprentissage numérique. Le service clientèle n'a accès aux données de l'école/de l'enseignant/de l'élève qu'à la demande de l'enseignant et avec l'autorisation expresse de celui-ci, dans le but exclusif de prêter assistance à l'utilisateur final.	Actes administratifs dans le cadre de l'exploitation des outils d'apprentissage, des systèmes d'administration scolaire, des commandes et des licences Assistance à l'utilisateur final
Les analystes/experts qui développent le matériel didactique ont accès à des ensembles de résultats anonymisés découlant de l'utilisation des outils d'apprentissage/systèmes d'administration scolaire.	Analyse du matériel didactique dans le but d'améliorer le matériel, de développer et d'optimiser le matériel didactique adaptatif, de contrôler et d'améliorer la qualité du matériel
Analyse du matériel didactique dans le but d'améliorer le matériel, de développer et	Les actes des administrateurs des bases de données informatiques visent la continuité et la gestion des systèmes TIC.

d'optimiser le matériel didactique adaptatif, de contrôler et d'améliorer la qualité du matériel	

II. Description générale des mesures destinées à protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites

Organisation de la sécurité des informations et procédures de communication

- Plantyn SA dispose d'un coordinateur de la protection de l'information chargé d'identifier les risques liés au traitement des données à caractère personnel, de sensibiliser à la sécurité, de surveiller les équipements et de prendre des mesures dans le but de garantir le respect de la politique de protection de l'information.
- Les incidents de protection de l'information sont documentés et servent à optimiser la politique de protection de l'information.
- Plantyn SA a élaboré une procédure pour communiquer à propos des incidents de protection de l'information.

Collaborateurs

- Des accords de confidentialité et des accords de protection de l'information sont conclus avec les collaborateurs.
- Plantyn SA favorise la sensibilisation, l'éducation et la formation en matière de protection de l'information.
- La catégorisation des collaborateurs permet de s'assurer que ceux-ci n'ont pas accès à plus de données que strictement nécessaire dans le cadre de leur fonction.

Sécurité physique et continuité des outils

- Les données à caractère personnel sont traitées exclusivement dans un environnement fermé, physiquement sécurisé et protégé contre les menaces externes.
- Les données à caractère personnel sont traitées exclusivement sur un équipement ayant fait l'objet de mesures visant à le sécuriser physiquement et à assurer la continuité du service.
- Des back-up sont réalisés périodiquement afin d'assurer la continuité du service. Ces back-up sont traités en toute confidentialité et sont conservés dans un environnement fermé.
- Les sites sur lesquels sont traitées les données font périodiquement l'objet de tests, de travaux de maintenance et d'évaluations quant aux risques en matière de sécurité. Plantyn SA dispose de plans de continuité des activités prévoyant des sites de reprise après sinistre.

Sécurité et maintenance des réseaux, des serveurs et des applications

- L'environnement réseau dans lequel sont traitées les données est strictement sécurisé. Les flux de trafic sont séparés, et des mesures sont mises en œuvre contre les abus et les attaques.
- L'environnement dans lequel les données à caractère personnel sont traitées est surveillé.

- Les outils d'apprentissage numériques dans lesquels sont traitées des données à caractère personnel reposent sur la conception du système, le contrôle de la sécurité et l'acceptation. Les modifications apportées aux applications sont testées afin de détecter leurs vulnérabilités avant la mise en production.
- Les correctifs (de sécurité) les plus récents sont installés périodiquement sur les systèmes, conformément à la gestion des correctifs.
- Les données traitées dans les applications sont classées en fonction des risques.
- Périodiquement, des tests d'intrusion et des évaluations de la vulnérabilité sont réalisés.
- Les informations qui ne sont pas (ou qui ne sont plus) utilisées sont supprimées.
- Des mesures cryptographiques sont appliquées aux mots de passe afin de conserver ces données en toute sécurité.
- Les communications utilisées pour les processus de connexion sont cryptées. L'échange de données à caractère personnel avec des tiers pour le compte de l'établissement d'enseignement est crypté.

III. Description générale de la politique de protection de l'information et des mesures permettant d'une part d'identifier les vulnérabilités relatives au traitement des données à caractère personnel dans les systèmes qui servent à la fourniture des services destinés à l'établissement d'enseignement et permettant d'autre part de remédier à ces vulnérabilités

La sécurité des systèmes de Plantyn SA fait l'objet de contrôles réguliers. En outre, la politique de sécurité de Plantyn SA prévoit des processus internes pour identifier les vulnérabilités.

Notification des violations de données à caractère personnel

Notification en cas de violation de données à caractère personnel et/ou d'incidents de sécurité. Si et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

- Les informations relatives à un incident qui doivent être partagées dans tous les cas pour permettre au responsable du traitement de se conformer à l'obligation de notification auprès de l'Autorité de protection des données. Les éléments figurant en gras doivent toujours être communiqués en cas de violation de données à caractère personnel.
    - Les caractéristiques de l'incident, comme la date et l'heure de la constatation, le résumé de l'incident, la caractéristique et la **nature de l'incident** (comment s'est-il produit ? S'agit-il d'une lecture, d'une copie, d'une modification, d'une suppression/destruction et/ou d'un vol de données à caractère personnel ?)
    - La **cause** de l'incident de sécurité
    - Les **mesures** prises pour gérer l'incident et pour limiter et prévenir les dommages éventuels/ultérieurs
    - Identifier les **personnes concernées** susceptibles d'être affectées par l'incident et la mesure dans laquelle elles risquent d'être affectées
    - La **taille du groupe de personnes concernées**

- Le **type de données** concernées par l'incident (notamment les données particulières ou sensibles, dont les données d'accès ou d'identification, les données financières ou les résultats d'apprentissage)
- Le **volume des données**
- Les **conséquences probables pour les personnes concernées**

Version

La dernière mise à jour de la présente annexe date du 17 mai 2018.