Itslearning AS
P.O. Box 2686
5836 Bergen
Norvège

tél. :+47 55 23 60 70
e-mail :post@itslearning.com

Accord avec le Sous-traitant en matière de traitement des données

ENTRE LES SOUSSIGNÉS

[INDIQUER LE NOM DU CLIENT] …….
SOC. Nº [INDIQUER LE NUMÉRO D'IMMATRICULATION DE LA SOCIÉTÉ]…….
(CI-APRÈS DÉNOMMÉE « LE RESPONSABLE DU TRAITEMENT»)
ET
ITSLEARNING AS, DONT LES DONNÉES D'IDENTIFICATION FIGURENT DANS L'ACCORD DE SOUSCRIPTION DE SERVICES STANDARD (CI-APRÈS DÉNOMMÉE LE « SOUS-TRAITANT »)

1. Objet

L'objet du présent accord est de règlementer les droits et les obligations énoncés dans la législation européenne sur la protection des données, et notamment dans la RGPD (ci-après dénommée la « Règlementation applicable en matière de protection des données »), à laquelle est soumis le Responsable du traitement dans le cadre de l'accord de souscription de services standard (ci-après dénommé l'« Accord de souscription »).

Cet accord vise à garantir que les données à caractère personnel dont le traitement est réalisé dans le cadre de l'Accord de souscription (https://itslearning.com/fr/cgv/) ne sont pas utilisées illégalement ni n'arrivent entre les mains de tiers non autorisés à cet effet.

Les notifications réalisées dans le cadre du présent accord doivent être réalisées auprès de la personne de contact indiquée dans le bon de commande.

Toute demande de renseignement ou requête du Responsable du traitement en lien avec les services fournis dans le cadre de cet accord doit être adressée au délégué à la protection des données du Sous-traitant :

Riikka Turunen
Sanoma Media Finland Oy
+35 89 122 4791
privacyteam@sanoma.com

2. Définitions

La RGPD désigne le 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, abrogeant la Directive 95/46/CE.

Les autres termes et concepts en lien avec la protection des données utilisés dans le cadre du présent accord ont le même contenu et le même sens que ceux figurant dans la RGPD.

3. Traitement et responsabilité principale

Le présent accord règlemente le traitement des données à caractère personnel par le Sous-traitant pour le compte du Responsable du traitement, y compris la collecte, l'enregistrement, le rapprochement, le stockage et la diffusion ou une combinaison de ces actions. L'objet et les détails concernant les données à caractère personnel traitées sont exposés dans l'annexe 1.

Le Sous-traitant n'a pas le droit de disposer lui-même des données à caractère personnel et il ne peut les traiter à ses propres fins. Les données à caractère personnel ne peuvent être utilisées que pour satisfaire aux conditions de l'Accord de souscription, dans le respect des limites fixées par le Responsable du traitement.

Si le Sous-traitant se voyait obligé par la loi à procéder au traitement de données à caractère personnel d'une façon différente de celle indiquée par le Responsable du traitement, le Sous-traitant devrait le notifier au Responsable du traitement avant de commencer l'opération, à moins que la législation applicable ou une quelconque juridiction ne l'en empêche.

4. Fonctions et responsabilités du Responsable du traitement

Le Responsable du traitement a la responsabilité de veiller à l'existence d'une base légale justifiant le traitement des données à caractère personnel, et au respect de la Législation applicable en matière de protection des données dans le cadre dudit traitement.

En vertu de cette responsabilité qui lui incombe, le Responsable du traitement est tenu de s'assurer que l'/les administrateur(s) du système détient/détiennent les autorisations nécessaires avant de procéder au traitement de données à caractère personnel pour le compte du Responsable du traitement.

Le Responsable du traitement effectuera également les évaluations nécessaires de l'impact du traitement sur la protection des données et la confidentialité, c'est-à-dire une évaluation de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel, préalablement à leur démarrage.

Le Responsable du traitement a la responsabilité de traiter les requêtes adressées par les utilisateurs finaux en vue d'accéder aux données à caractère personnel détenues par le Responsable du traitement ou par le Sous-traitant en vertu de l'accord. Dans le cas de recevoir une requête de ce type, le Sous-traitant doit recommander à l'utilisateur final correspondant d'adresser sa requête au Responsable du traitement, auquel incombe la responsabilité d'y répondre.

L'Accord de souscription autorise le Responsable du traitement à installer et à activer des produits supplémentaires de tiers externes (y compris les extensions). Le Responsable du traitement reconnaît que s'il installe, utilise ou active les produits de ces tiers, leur donnant ainsi accès aux

données à caractère personnel, le présent accord avec le Sous-traitant en matière de traitement des données n'est pas applicable au traitement des données transmises à ou par ces produits de tiers externes. Le Responsable du traitement peut activer ou désactiver l'utilisation de produits de tiers externes, et il n'est pas tenu d'utiliser de tels produits dans le cadre de l'Accord de souscription.

5. Fonctions et obligations du Sous-traitant

Le Sous-traitant doit uniquement procéder au traitement des données à caractère personnel pour le compte du Responsable du traitement et en respectant strictement les consignes de ce dernier. Le traitement à titre secondaire des données à caractère personnel par le Sous-traitant visant à assurer la sécurité, la maintenance courante, l'analyse ou l'évaluation des services fournis dans le cadre de l'Accord de souscription et n'ayant pas d'impact défavorable sur le niveau de protection des données des personnes concernées n'est pas considéré comme constituant un traitement par le Sous-traitant à ses propres fins.

Le Sous-traitant s'engage à donner accès au Responsable du traitement à toutes les informations nécessaires, à justifier du respect de la Législation applicable en matière de protection des données, et à fournir son assistance au Responsable du traitement pour lui permettre de s'acquitter des responsabilités qui lui incombent au regard de la loi et de la règlementation.

Sauf convention contraire ou sauf exigences légales contraires, le Responsable du traitement possède un droit d'accès aux données à caractère personnel traitées par le Sous-traitant pour le compte du Responsable du traitement et à tous les systèmes utilisés à cet effet. Le Sous-traitant s'engage à lui prêter son assistance en ce sens. Toutefois, le Sous-traitant ne peut pas être contraint à transmettre au Responsable du traitement des informations professionnelles confidentielles ou commercialement sensibles. En outre, le Responsable du traitement ne possède pas de droit d'accès si cela implique un risque pour la sécurité ou l'intégrité de données à caractère personnel en question.

Le Sous-traitant, y compris les employés de celui-ci, est tenu à un devoir de confidentialité concernant les documents et les données à caractère personnel auxquels le Sous-traitant a accès en vertu du présent accord. Cette disposition demeure applicable même après la fin de cet accord. Tous les accords de confidentialité nécessaires doivent être signés avec les employés qui ne sont pas déjà soumis à une obligation légale de confidentialité ou de secret. L'obligation de confidentialité concerne également les employés des sous-traitants qui réalisent la maintenance (ou autres tâches semblables) des systèmes auxquels le Sous-traitant fait appel pour fournir ou gérer le service.

Les politiques et processus d'accès aux données internes des sous-traitants sont conçus pour empêcher l'accès des personnes et/ou systèmes non autorisés aux systèmes utilisés pour le traitement des données à caractère personnel. Le Sous-traitant conçoit ses systèmes de manière à ce que seules les personnes autorisées à accéder aux données puissent le faire et de façon à s'assurer que les données à caractère personnel ne puissent pas être lues, copiées, modifiées ni supprimées sans autorisation lors de leur traitement, de leur utilisation et après leur enregistrement. La gestion des autorisations est assurée par des outils de workflow qui tiennent des registres de vérification de tous les changements. L'accès aux systèmes se fait via l'ouverture de sessions, afin de créer un historique permettant d'en rendre compte. Le détail des sessions ouvertes doit être conservé par le Sous-traitant pendant un minimum de 3 mois. Le Responsable du traitement doit pouvoir avoir accès au détail des sessions ouvertes s'il en fait la demande.

6. Délégué à la protection des données

Le Sous-traitant a désigné un délégué à la protection des données, conformément aux exigences de la Législation applicable en matière de protection des données.

7. Recours à des sous-traitants et exportation des données

Pour avoir recours à d'autres sous-traitants en vue du traitement des données à caractère personnel, le Sous-traitant doit avoir reçu au préalable l'autorisation écrite du Responsable du traitement, sauf si le recours à la sous-traitance est déjà prévu dans l'Accord de souscription. Le Sous-traitant est tenu de s'assurer que l'accès par ses propres sous-traitants aux données à caractère personnel et leur utilisation sont conformes aux conditions du présent Accord avec le Sous-traitant en matière de traitement des données et que les sous-traitants en question ont signé les accords écrits correspondants les contraignant à offrir au minimum le niveau de protection des données demandé par la Législation applicable en matière de protection des données. Pour des motifs raisonnables et justifiables, le Responsable du traitement peut refuser d'autoriser de nouveaux sous-traitants.

Les sous-traitants figurant sur la liste du site web suivant ont reçu l'autorisation du Responsable du traitement aux fins du présent accord : https://itslearning.com/global/gdpr/subprocessors. Si le Responsable du traitement avait besoin de plus d'informations détaillées sur les lieux où se déroule le traitement en vue du respect des exigences légales des autorités de protection des données, le Sous-traitant devrait aider le Responsable du traitement à faire face à ce besoin en matière de conformité, à condition que, préalablement à cette transmission d'informations, le Responsable du traitement ait contracté les obligations de confidentialité pertinentes, si le Sous-traitant l'a jugé nécessaire.

Les changements en lien avec l'ajout ou le remplacement d'une société figurant dans la liste mentionnée précédemment doivent être portés à la connaissance du Responsable du traitement, notamment en les annonçant via des avis automatiques ou par d'autres moyens appropriés, le cas échéant. Dans les 4 semaines suivant la réception de l'avis, le Responsable du traitement peut contester le changement ou l'ajout, mais seulement pour des motifs raisonnables.

Le Sous-traitant a la responsabilité face au Responsable du traitement des actions et omissions de ses sous-traitants, celles-ci étant considérées comme des actions ou omissions du Sous-traitant lui-même. Le Sous-traitant a la responsabilité de s'assurer que ses sous-traitants connaissent bien les obligations contractuelles et légales qui incombent au Sous-traitant et qu'ils s'en acquittent d'une façon semblable à la sienne.

Le Sous-traitant et ses éventuels sous-traitants ne peuvent pas diffuser les données à caractère personnel hors de la zone UE et de l'EEE ou de pays tiers préalablement autorisés sans avoir avant obtenu l'autorisation écrite du Responsable du traitement. L'accès à ou l'utilisation par le Responsable du traitement de données à caractère personnel depuis un pays tiers ou au sein de celui-ci n'est pas, pour le compte du Sous-traitant ou de l'un des sous-traitants de ce dernier, considéré comme un transfert de données à caractère personnel vers ce pays tiers.

Lorsqu'un tel transfert de données à caractère personnel a lieu, soit vers des sociétés de traitement de données ou d'autres tiers sous-traitants situés dans des pays hors UE/EEE, il doit être soumis à des mécanismes de transfert appropriés et contraignants, offrant un degré satisfaisant de protection conformément aux dispositions de la Législation applicable en matière de protection des données.

8. Sécurité

a. Mesures de sécurité et documents

Le Sous-traitant doit respecter les exigences concernant les mesures de sécurité stipulées par la Législation applicable en matière de protection des données. Le Sous-traitant a l'obligation de rendre compte par écrit des mesures de sécurité adoptées. L'annexe 3 contient un aperçu des mesures de sécurité à adopter par le Sous-traitant. Le Responsable du traitement peut avoir accès sur demande à des documents plus détaillés.

Le Sous-traitant doit mettre en place et maintenir les mesures de sécurité appropriées au niveau technique et organisationnel permettant de garantir un niveau de sécurité à la hauteur des risques courus, en tenant notamment compte de la nature de tous les services en nuage fournis au Responsable du traitement. Ces mesures doivent protéger les données à caractère personnel de la destruction accidentelle ou illicite, de la diffusion non autorisée ou de l'accès aux données à caractère personnel transmises, stockées ou ayant fait l'objet de tout autre type de traitement. En établissant ces mesures, le Sous-traitant doit tenir compte du caractère confidentiel, de l'intégrité, de la disponibilité et de la résilience de l'information et des services et systèmes de traitement.

Dans le cadre du traitement des données à caractère personnel, les mesures de sécurité appropriées doivent inclure, entre autres, suivant le cas :

- La pseudonymisation et le cryptage des données à caractère personnel.
- La capacité de garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement.
- La capacité de restaurer la disponibilité des données à caractère personnel et l'accès à celles-ci de façon rapide en cas d'incident technique ou physique.
- Un processus permettant de tester, examiner et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement des données.

Le Responsable du traitement et le Sous-traitant doivent prendre des mesures pour garantir que quiconque agissant sous l'autorité du Responsable du traitement et du Sous-traitant et ayant accès aux données à caractère personnel procède à leur traitement en tenant exclusivement compte des consignes du Responsable du traitement, sauf en cas d'être tenu au contraire, en vertu de la Législation applicable en matière de protection des données ou de toute autre législation.

b. Aperçu des activités de traitement

Le Sous-traitant, et, le cas échéant, son délégué, est tenu de tenir et conserver une liste de toutes les catégories d'activités de traitement réalisées pour le compte du Responsable du traitement, en indiquant :

a) Le nom et les coordonnées du Sous-traitant et du délégué à la protection des données.
b) Les catégories de traitement menées à bien pour le compte du Responsable du traitement.
c) Le cas échéant, les transmissions de données à caractère personnel vers des pays hors UE/EEE, en identifiant le pays tiers en question et en incluant les documents concernant des mesures de protection pertinentes, selon les besoins.

d) Si possible, une description générale des mesures de sécurité techniques et organisationnelles appliquées.
La liste doit être tenue à jour conformément aux dispositions de la clause 9 ci-après. Le Sous-traitant doit mettre cette liste à la disposition des autorités de protection des données correspondantes, à la demande de ces dernières.

c. Notification concernant la violation des données

Toute violation des données compromettant la sécurité ou la confidentialité des données à caractère personnel doit être signalée au point de contact indiqué au point 1 du présent accord. Cette notification doit être émise dans les meilleurs délais, et dans tous les cas dans les 72 heures après que le Sous-traitant a pris connaissance de cette violation.
La notification doit contenir :

- Une description des données à caractère personnel et, si possible, du type et du nombre de personnes affectées ainsi que du type et de la quantité de données à caractère personnel compromises.
- Le nom et les coordonnées d'un délégué à la protection des données ou autre personne de contact.
- Une description des conséquences susceptibles d'être entraînées par l'incident.
- Une description des mesures prises ou proposées pour faire face à l'incident et, le cas échéant, les mesures pour réduire ses possibles effets négatifs.

Le Responsable du traitement a la responsabilité de notifier formellement une violation importante de données à caractère personnel aux autorités de protection des données et, le cas échéant, aux personnes affectées par cette violation.

d. Gestion de l'accès et équipements

Le Sous-traitant est tenu de s'assurer de la bonne sécurisation du service, y compris des serveurs, bases de données et autres équipements ou logiciels pertinents, de sorte qu'aucune personne non autorisée ne puisse avoir accès aux données à caractère personnel. Cela s'applique également aux copies papier et à tout autre document physique.

Par ailleurs, le Sous-traitant doit avoir mis en place un système de contrôle de sécurité conforme à la Législation applicable en matière de protection des données. Ce système doit inclure, à titre non exhaustif, des procédures pour :

- Le traitement des non-conformités, et notamment l'émission d'une notification concernant le mauvais usage du système d'information, et notamment les violations.
- Des contrôles de sécurité.

Le Sous-traitant doit établir et maintenir les mesures de sécurité dont le besoin a été détecté lors des évaluations du risque en matière de sécurité et de technologie.

9. Mise à jour des activités de traitement et des contrôles de sécurité

La liste des activités de traitement, cf. clause 8 b) ci-avant, doit être vérifiée et mise à jour au moins une fois par an ou après des changements importants dans ces activités.

Le Sous-traitant est tenu, au moins une fois par an ou à la suite d'anomalies ou de changements

importants, de mener régulièrement à bien des contrôles de sécurité sur les systèmes et toute autre démarche pertinente en vue du traitement des données à caractère personnel dans le cadre du présent accord. Lors du contrôle de sécurité, il faut s'assurer que les mesures techniques, physiques et organisationnelles qui ont été définies sont respectées et produisent les effets désirés, en identifiant les éventuelles améliorations à apporter.

Le Sous-traitant doit rendre compte par écrit des résultats du contrôle de sécurité et mettre ces conclusions à la disposition du Responsable du traitement, afin que celui-ci puisse, entre autres, les utiliser dans ses propres contrôles de sécurité.

Les systèmes et processus du Sous-traitant doivent faire régulièrement l'objet de vérifications et certifications, et les certifications applicables doivent être fournies au Responsable du traitement à la demande de celui-ci.

Les dépenses supplémentaires découlant des vérifications spéciales demandées ou réalisées par le Responsable du traitement sont à la charge du Responsable du traitement.

10. Durée de l'accord

L'accord produit ses effets à compter du 25 mai 2018 ou à compter de la date dont les parties pourraient convenir, à condition qu'elle soit postérieure au 25 mai 2018, et ceci pendant toute la durée de l'Accord de souscription. Il annule et remplace tout Accord avec le Sous-traitant en matière de traitement des données qui aurait été signé par les parties avant cette date.

En cas de manquement au présent accord ou à la Législation applicable en matière de protection des données, le Responsable du traitement peut demander au Sous-traitant de mettre un terme au traitement des données à caractère personnel.

11. Retour et effacement au terme de l'accord

Au terme de l'accord, le Sous-traitant est tenu de remettre, réécrire, effacer, cf. Procédures d'effacement prévues à l'annexe 2, et/ou détruire correctement tous les documents, supports de stockage et tout autre élément contenant des données à caractère personnel s'inscrivant dans le cadre du présent accord. Cela s'applique aussi à toutes les copies de sauvegarde. Le Sous-traitant doit rendre compte par écrit de la réalisation de ces mesures conformément au présent accord dans un délai raisonnable après la fin de cet accord.

Tous les coûts liés à l'exécution de cette clause sont à la charge du Responsable du traitement, sauf indication contraire dans l'Accord de souscription.

12. Loi applicable et juridiction compétente

La loi applicable et la juridiction compétente sont celles prévues dans l'Accord de souscription ou celles dont pourraient convenir les parties au présent accord.

***

Pour **itslearning** **(LE SOUS-TRAITANT)**	Pour le **Client** **(LE RESPONSABLE DU TRAITEMENT)**
Nom du signataire d'itslearning :	Nom du signataire du Client :
Signé :	Signé :
Nom :	Nom :
Poste :	Poste :
Date :	Date :

ANNEXE 1

Objet et détails concernant les données à caractère personnel traitées Motif et objectifs du traitement

En tant que Sous-traitant, itslearning procède au traitement des données à caractère personnel reçues dans le cadre du Service (c'est-à-dire via le logiciel d'itslearning), via le service hébergé pour le Client, via les applications de partenaires et le site web (http://www.itslearning.com), et ceci pour le compte du Responsable du traitement et aux fins suivantes :

- Prestation des services conformément à l'Accord avec le Sous-traitant en matière de traitement des données et à l'Accord de souscription.
- Fourniture d'un support technique et de base en lien avec les Services, conformément à l'Accord avec le Sous-traitant en matière de traitement des données et à l'Accord de souscription de services standard.
- Sauvegarde des données du Responsable du traitement.
- Le Sous-traitant peut recueillir des informations sur l'utilisation du Service par le Responsable du traitement en vue de l'élaboration de statistiques internes et de factures.

Durée du traitement

Elle couvre la durée de l'Accord de souscription, plus la période allant de l'échéance de cet accord à l'effacement de toutes les données du Client par le Sous-traitant, conformément aux conditions établies.

Catégories de données à caractère personnel

Le Sous-traitant procède au traitement des données à caractère personnel transmises, stockées, importées, envoyées ou reçues dans le cadre du Service, par le (ou sur les instructions du) Responsable du traitement et ses utilisateurs autorisés. L'étendue des données est définie et contrôlée à l'entière discrétion de ces personnes. Les données appartiennent aux catégories suivantes :

- Coordonnées et identification (nom, e-mail, numéro de téléphone, adresse, nom d'utilisateur, etc.)
- Coordonnées des parents ou tuteurs
- Communications (messages entre utilisateurs, discussions, commentaires de publications, notifications, etc.)
- Contenus de cours
- Évaluations, résultats d'évaluations et notes
- Evénements calendaires
- Documents, présentations, images, devoirs, taches, etc.

Personnes concernées

Le traitement des données à caractère personnel par le Sous-traitant dans le cadre du Service pour le compte du Responsable du traitement peut inclure, à titre non exhaustif, les données à caractère personnel en lien avec les catégories de personnes concernées suivantes :

- Les employés du Client, et notamment les enseignants, administrateurs, intervenants, tuteurs et autres.
- Les autres employés et prestataires du Client, et tout autre utilisateur autorisé par le client, qui transmettent des données à caractère personnel dans le cadre du Service, y compris les apprenants et leurs parents.

ANNEXE 2 | PROCÉDURES D'EFFACEMENT

Effacement des données au terme de l'accord

Dans les 6 mois suivant la fin de l'accord entre le Responsable du traitement et le Sous-traitant, toutes les données traitées pour le compte du Responsable du traitement doivent être effacées de façon définitive, y compris les copies de sauvegarde.

Retrait de supports de stockage et politique d'effacement

Les supports de stockage/disques (y compris les lecteurs de disque dur, les disques SSD, les clés USB et les cassettes) contenant des données sont susceptibles de présenter des problèmes d'utilisation, des erreurs ou des pannes entraînant leur retrait. Tous les supports de stockage retirés sont soumis à une série de processus de destruction des données avant leur sortie des installations du Sous-traitant, que ce soit en vue de leur réutilisation ou de leur destruction, conformément à notre « Politique d'entreprise – Destruction des supports de stockage », afin de veiller à ce que toutes les données soient complètement effacées et détruites, et ceci de façon sûre. Les résultats des effacements sont enregistrés sous le numéro de série du support de stockage retiré, en vue de leur suivi.

ANNEXE 3 | MESURES DE SÉCURITÉ

itslearning a mis en place les mesures de sécurité détaillées dans la présente annexe, au niveau organisationnel et technique, conformément aux normes du secteur. itslearning est susceptible de mettre à jour ou modifier ces mesures de sécurité de temps à autre, à condition de ne pas entraîner de dégradation de la sécurité générale des services. La toute dernière version peut être consultée sur https://itslearning.com/global/gdpr/securitymeasures.

Mesures organisationnelles

L'équipe de direction d'itslearning s'est impliquée activement dans le développement d'une culture de la sécurité de l'information au sein de l'entreprise, par le biais d'un programme continu de sensibilisation, et une structure a été mise en place en son sein pour gérer la sécurité de l'information dans ses services, avec une définition claire des fonctions et responsabilités au sein de l'organisation. En 2019, itslearning a débuté un long processus de certification avant de se voir remettre la certification ISO 27 001 le 11 mars 2020.

Gestion des opérations

Il existe de nombreuses procédures et politiques de bonnes pratiques du secteur visant à garantir la meilleure confidentialité, disponibilité et intégrité possibles de la plate-forme. Ces politiques sont axées sur des exigences strictes dans une multitude de domaines tels que :

- La sécurité de l'information.
- La sécurité des environnements d'hébergement.
- L'accès à des services tiers.
- Le contrôle de la capacité.
- La conduite du changement.
- La sauvegarde et la restauration.
- Le contrôle des accès.
- La documentation.
- L'identification lors des sessions et la surveillance.
- Les réponses en cas d'incident.
- La gestion des mises en production.

Équipe de sécurité

itslearning possède une équipe d'experts en sécurité, en charge de la sécurité générale des informations au sein de l'entreprise. Ils sont entre autres responsables de :

- La coordination des tâches en matière de sécurité.
- La sécurisation de l'environnement, des réseaux et appareils de l'entreprise.
- La sécurité de l'application (tests de pénétration internes et vérifications de l'application).
- La surveillance et l'identification lors de l'ouverture des sessions.
- La gestion des processus et des politiques (plan anti-sinistre, gestion des chemins d'accès, etc.).
- La formation des employés dans le domaine de la sécurité de l'information.

- La coordination du contrôle de la sécurité des services tiers et le suivi des résultats de ce contrôle.
- La revue du code face à d'éventuelles failles de sécurité.

Fonctions et responsabilités

Tous les employés exercent des fonctions clairement définies au sein de l'entreprise, et leur accès aux données n'a lieu que dans le cadre de l'exercice de ces fonctions spécifiques. Un nombre limité d'employés a un accès administratif à notre environnement de production et leurs droits sont strictement règlementés et régulièrement réexaminés. Tout changement important dans l'application, l'environnement ou les équipements de l'environnement de production fait toujours l'objet de vérification de la part d'au moins deux personnes.

Sécurité du personnel

Tout le personnel d'itslearning signe un accord de confidentialité très strict. Il est tenu de respecter les politiques définies par l'entreprise en matière de confidentialité, de déontologie et de normes professionnelles. Les membres du personnel chargés de sécuriser, manipuler et traiter les données des clients suivent une formation appropriée pour l'exercice de ces fonctions.

Contrôle des accès

Des exigences strictes sont en place pour les employés, consultants extérieurs ou tiers ayant besoin d'accéder aux systèmes d'information d'itslearning. Le contrôle des accès est assuré via un système d'authentification. L'utilisateur doit ainsi :

- Avoir reçu l'autorisation d'accéder de la part de la direction.
- Avoir des mots de passe sûrs conformes à la politique de l'entreprise en la matière.
- Changer régulièrement de mot de passe.
- Justifier que l'accès demandé est nécessaire pour l'exercice de ses fonctions/sa mission spécifiques.
- Veiller à ce que l'appareil (PC, tablette, téléphone portable) utilisé soit dûment sécurisé et verrouillé en son absence.

itslearning fait appel à un verrouillage automatique temporaire de l'appareil de l'utilisateur si celui-ci n'est pas en cours d'utilisation.

Les politiques et processus d'accès aux données internes des sous-traitants sont conçus pour empêcher l'accès des personnes et/ou systèmes non autorisés aux systèmes utilisés pour le traitement des données à caractère personnel. Tout changement introduit dans les données est enregistré afin de créer un historique permettant d'en rendre compte.

Sécurité physique

a. Centres de données

itslearning gère tous les services fournis à ses clients depuis des centres de données séparés de l'espace de travail situé dans les bureaux de l'entreprise. L'accès aux centres de données fait l'objet d'un contrôle et d'une protection stricts, afin de réduire les possibilités d'accès non autorisé, les incendies, inondations ou tout autre dommage sur l'environnement physique. L'accès physique aux centres de données est limité à un nombre réduit d'employés d'itslearning ou des fournisseurs des centres d'hébergement. Des

autorisations de sécurité strictes sont exigées et doivent être validées par le service de sécurité, avant d'accéder au centre de données.

b. Bureaux

Tous les bureaux d'itslearning sont protégés par un contrôle d'accès. Seuls les visiteurs invités et les employés peuvent accéder aux bureaux d'itslearning. De nombreuses mesures sont en place pour éviter les problèmes de sécurité liés à de possibles vols ou pertes d'équipements informatiques. Cela inclut des consignes de sécurité et l'acceptation de politiques d'utilisation, des systèmes d'authentification et le cryptage des unités de stockage, s'il y a lieu.

Mesures techniques

Disponibilité du système

itslearning a mis en place des mesures conformes aux normes du secteur afin de garantir que les données à caractère personnel soient protégées des destructions ou pertes accidentelles, et notamment :

- La redondance des infrastructures (entre autres de la totalité du réseau, des installations électriques, de refroidissement, des bases de données, du serveur et de stockage).
- Les copies de sauvegarde sont stockées à un autre endroit et peuvent être récupérées en cas de panne du système principal.
- Protection appropriée contre le déni de service.
- Personnel disponible 365 jours par an, 24 h/24 et 7 j/7 pour assurer la surveillance et le dépannage.

Protection des données

itslearning a mis en place une série de mesures conformes aux normes du secteur afin d'empêcher que les données à caractères personnelles soient lues, copiées, modifiées ou effacées par des parties non autorisées au cours d'un transport ou sur place. Ces mesures comprennent :

- L'utilisation de pare-feu multicouches, de VPN et de technologies de cryptage pour protéger les passerelles et pipelines.
- Le cryptage HTTPS (également appelé SSL ou TLS) à l'aide de clés cryptographiques sûres.
- L'accès à distance aux centres de données est protégé par un certain nombre de couches réseau de sécurité.
- Les données particulièrement sensibles de clients sont protégées sur place par le cryptage et/ou le hachage (pseudonymisation).
- Tous les disques retirés sont soumis à des procédures d'effacement conformément à notre « Politique d'effacement de disque », et le retrait est enregistré sous le numéro de série du disque.
- Des vérifications régulières de la sécurité des services tiers (au moins une fois par an), comprenant des tests de pénétration, consultables par les clients.

Centres de données

itslearning n'utilise que des centres de données de pointe, qui assurent la sécurité et la surveillance sur place 365 jours par an, 24 h/24 et 7 j/7. Les centres de données sont situés dans des installations modernes résistantes aux incendies, demandant un accès électronique par carte-clé, avec des alarmes reliées au système de sécurité sur place. Seuls les employés et les prestataires autorisés peuvent demander l'accès électronique par carte-clé à ces installations.

Système de développement

La plate-forme d'itslearning est basée sur des technologies conformes aux normes du secteur offertes par des fournisseurs reconnus, comme Microsoft, Linux, Dell, Fujitsu, Amazon, Cloudflare, F5 et Cisco. Les systèmes sont régulièrement mis à jour avec la dernière version, afin de pouvoir appliquer les dernières améliorations en matière de sécurité. En général, la plate-forme est mise à jour plusieurs fois par trimestre. La correction des erreurs se fait dans les meilleurs délais par ordre de priorité, et elle donne ensuite lieu à des contrôles de qualité rigoureux.

itslearning a mis en place des mesures permettant de réduire les risques d'intrusion dans le code de sa plate-forme susceptible de porter atteinte à la sécurité ou à l'intégrité des services client et des données à caractère personnel traitées. Ces mesures comprennent entre autres :

- La formation régulière du personnel.
- La révision de code par les architectes de sécurité.
- Les processus de qualité en vue de tester rigoureusement les changements avant leur mise en place.

Sécurité des sous-traitants

Pour le recrutement des sous-traitants, itslearning procède à un contrôle des pratiques de ces derniers en matière de sécurité et confidentialité, afin de garantir qu'ils offrent un niveau de sécurité et de confidentialité adapté à l'accès aux données et à la portée des services qu'ils devraient fournir. itslearning mène régulièrement à bien des contrôles de sécurité des pratiques et activités des actuels sous-traitants.