

Politique de Confidentialité et

De Protection Des Données

Cet accord de protection des données (le « APD ») entre en vigueur le 25 mai 2018.

Le client doit mettre à la disposition de ID-TRACKING et le client autorise ID-TRACKING à traiter des informations, y compris des données personnelles, en vue de la fourniture des services dans le cadre du contrat. Les parties ont convenu de conclure cet APD afin de confirmer les dispositions relatives à la protection des données relatives à leurs relations et de satisfaire aux exigences de la loi sur la protection des données applicable.

1. Définitions

1.1. Aux fins de cet APD :

" **Données personnelles** " désigne toute information concernant une personne physique identifiée ou identifiable (« personne concernée »); une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques au physique, au physiologique, identité génétique, mentale, économique, culturelle ou sociale de cette personne physique;

« **Loi sur la protection des données** » désigne toutes les lois, réglementations et autres exigences légales applicables concernant (a) la confidentialité, la sécurité des données, la protection des consommateurs, le marketing, la promotion, la messagerie texte, le courrier électronique et autres communications ; et (b) l'utilisation, la collecte, la conservation, le stockage, la sécurité, la divulgation, le transfert, la destruction et tout autre traitement de données à caractère personnel.

« **Les filiales de ID-TRACKING** » désigne toute entité qui, directement ou indirectement, contrôle, est contrôlée ou est sous contrôle commun avec ID-TRACKING. « **Contrôle** » aux fins du présent définition, signifie la propriété directe ou indirecte ou le contrôle de plus de 50% des droits de vote de l'entité visée ;

« **Services** » désigne l'un des services suivants fournis par ID-TRACKING :

(a) des offres de produits de marque de la Société ID-TRACKING mises à disposition sur le site Web de la Société ID-TRACKING,

(b) des services de conseil ou de formation fournis par ID-TRACKING à distance, via Internet ou en personne.

(c) tous les services de support fournis par ID-TRACKING, y compris l'accès au service d'assistance de ID-TRACKING ;

Les termes « **contrôleur de données** », « **traitement de données** », « **personne concernée** », « **données personnelles** », « **traitement** » et « **appropriée** » **mesures techniques et organisationnelles** » auront la signification qui leur est donnée en vertu de la loi applicable sur la protection des données

2. Objet, nature et objet du traitement des données personnelles par ID-TRACKING

2.1. L'objet, la nature et la finalité du traitement des données à caractère personnel au titre de la présente APD sont la prestation des services par ID-TRACKING, telle que formulée par écrit par le client lors de son utilisation des services, à moins que la loi sur la protection des données n'y oblige. Dans ce cas, dans la mesure permise par la loi sur la protection des données, ID-TRACKING informera le client de cette obligation légale avant de procéder au traitement. ID-TRACKING ne doit collecter ou traiter des données à caractère personnel que pendant la période de prestation des services dans la mesure et de la manière nécessaires à la fourniture des services et conformément à la loi sur la protection des données et à la loi sur la protection des données applicable à ID-TRACKING.

3. durée

3.1. Le traitement des données personnelles sera effectué par ID-TRACKING tant que le compte de services du client existe ou est nécessaire à l'exécution des obligations et des droits entre ID-TRACKING et le client, sauf convention écrite contraire.

4. Type de données personnelles traitées

4.1. Le client peut soumettre des données personnelles du client aux services, dont la portée est déterminée et contrôlée par le client à sa seule discrétion, et qui peut inclure, sans toutefois s'y limiter, les catégories de données personnelles suivantes :

- **Information sur le compte.** Lorsque le client ouvre un compte de services, il est nécessaire que certaines informations telles que le nom et l'email. Le Client peut mettre à jour ou corriger ses informations et préférences de courrier électronique à tout moment en visitant le compte Services. ID-TRACKING peut fournir au client une assistance supplémentaire pour accéder, corriger, supprimer ou modifier les informations le client.

Fourni à ID-TRACKING et associés aux services de la clientèle compte. Pour protéger la sécurité, ID-TRACKING prend des mesures raisonnables (par exemple, demander toute information juridique) pour vérifier l'identité du client avant de procéder aux corrections. Le client est responsable du maintien du secret du mot de passe et des Services de la clientèle compte à tout moment.

- **Informations de profil supplémentaires.** Le client peut choisir de fournir des informations supplémentaires dans le cadre de son profil. Les informations de profil aident le client à obtenir plus des services. Il est le choix du client d'inclure des informations sensibles sur son profil.
- **Les autres informations.** Le client peut autrement choisir de fournir les informations de ID-TRACKING lorsque le client remplit un formulaire, effectue une recherche, met à jour ou ajoute des informations à son compte de services, répond à des sondages, publie des messages sur des forums communautaires, participe à des promotions ou utilise d'autres fonctionnalités de la plate-forme de services.

3. Obligations de ID-TRACKING

3.1. ID-TRACKING accepte et / ou garantit :

- (a) traiter les données personnelles uniquement pour le compte du client et conformément à ses instructions et aux APD ; s'il ne peut fournir cette conformité pour quelque raison que ce soit, il

s'engage à informer rapidement le client de son incapacité à se conformer, auquel cas le client est en droit de suspendre le transfert des données et / ou de mettre fin aux services ;

- (b) que toutes les données personnelles traitées pour le compte du client restent la propriété du client et / ou des personnes concernées ;
- (c) qu'il n'a aucune raison de croire que la législation qui lui est applicable l'empêche de respecter les instructions reçues du client et ses obligations en vertu de la APD et qu'en cas de modification de cette législation susceptible d'avoir un effet défavorable important sur: des garanties et des obligations fournies par la APD, elle notifiera rapidement la modification au client dès qu'elle en aura connaissance, auquel cas le client est en droit de suspendre le transfert des données et / ou de mettre fin aux services;
- (d) avoir mis en œuvre les mesures de sécurité techniques et organisationnelles spécifiées à l'annexe 1 avant de traiter les données à caractère personnel transférées ;
- (e) qu'il informera rapidement le client de :
 - Toute demande juridiquement contraignante de divulgation des données personnelles par un service répressif, sauf interdiction contraire, telle qu'une interdiction pénale permettant de préserver la confidentialité d'une enquête policière ;
 - Tout accès accidentel ou non autorisé ; et toute demande reçue directement des personnes concernées sans répondre à cette demande, à moins d'être autrement autorisée à le faire ;
- (F) traiter rapidement et correctement toutes les demandes du client relatives au traitement des données à caractère personnel faisant l'objet du transfert et se conformer aux conseils de l'autorité de contrôle en ce qui concerne le traitement des données transférées ;
- (g) à la demande du client, de soumettre ses installations de traitement de données à l'audit des activités de traitement couvertes par le APD ;
- (h) qu'en cas de sous-traitants, il en ait préalablement informé le client et obtenu son consentement écrit préalable ;
- (i) que les services de traitement par le sous-traitant seront effectués conformément à la section 7;
- (j) nommer un responsable de la protection des données qui exerce ses fonctions conformément à la loi sur la protection des données. Les coordonnées du responsable de la protection des données sont disponibles sur la page Web de ID-TRACKING.
- (k) de ne confier qu'à ces employés le traitement des données décrit dans le présent APD, qui ont été tenus à la confidentialité et ont déjà été familiarisés avec les dispositions de protection des données pertinentes pour leur travail. ID-TRACKING et toute personne agissant sous son autorité qui a accès aux données personnelles ne doivent pas traiter ces données, sauf instructions contraires du client, sauf si cela est requis par la loi sur la protection des données ;
- (l) contrôler périodiquement les processus internes pour s'assurer que le traitement dans le champ de responsabilité de ID-TRACKING est conforme aux exigences de la loi sur la protection des données et à la protection des droits de la personne concernée.

5. Obligations du client

5.1. Le client accepte et / ou garantit :

- (a) que le traitement, y compris le transfert lui-même, des données à caractère personnel a été et continuera à être effectué conformément aux dispositions pertinentes de la loi sur la protection des données et ne viole pas les dispositions pertinentes ;
- (b) qu'il a reçu pour instruction et pendant toute la durée des services de traitement de données à caractère personnel de charger ID-TRACKING de traiter les données à caractère personnel transférées uniquement pour le compte du client et conformément à la loi sur la protection des données et aux APD ;
- (c) que ID-TRACKING fournira des garanties suffisantes en ce qui concerne les mesures de sécurité techniques et organisationnelles spécifiées à l'annexe 1 du présent APD ;
- (d) qu'après évaluation des exigences de la loi sur la protection des données, les mesures de sécurité permettent de protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la divulgation non autorisée ou l'accès, en particulier lorsque le traitement implique la transmission de données sur un réseau et contre toutes les autres formes de traitement illicites, et que ces mesures assurent un niveau de sécurité approprié aux risques présentés par le traitement et à la nature des données à protéger, eu égard à l'état de la technique et au coût de leur mise en œuvre. ;
- (e) qu'il veillera au respect des mesures de sécurité ;
- (f) d'accéder aux Services et de les utiliser uniquement à des fins légales, autorisées et acceptables. Le client n'utilisera pas (ni n'assistera d'autres personnes dans l'utilisation) des services de manière à : (a) violer, détourner ou détourner les droits de ID-TRACKING, de ses utilisateurs ou de tiers, y compris la confidentialité, la publicité, la propriété intellectuelle ou d'autres droits exclusifs; droits; (b) sont illégaux, obscènes, diffamatoires, menaçants, intimidants, harcelants, haineux, offensants sur le plan racial ou ethnique, ou incitent ou encouragent un comportement qui serait illégal ou autrement inapproprié;
 - (c) impliquent la publication de faussetés, de fausses déclarations ou de déclarations trompeuses ;
 - (d) usurper l'identité de quelqu'un ;
 - (e) impliquent l'envoi de communications illégales ou non autorisées, telles que la messagerie groupée, la messagerie automatique, la numérotation automatique, etc. ou (f) impliquent toute autre utilisation des Services prescrits dans le présent APD, sauf autorisation contraire de ID-TRACKING ;
- (g) ne pas (ou aider d'autres personnes) à accéder, utiliser, copier, adapter, modifier, préparer des œuvres dérivées fondées sur, distribuer, concéder sous licence, concéder en sous-licence, transférer, afficher, exécuter ou exploiter de quelque manière que ce soit la plate-forme de services de manière non autorisée ou non autorisée, ou de manière à alourdir, altérer ou nuire à ID-TRACKING, à la plate-forme de services, aux systèmes, aux autres utilisateurs ou à d'autres, y compris le fait que le client ne veut pas, directement ou par des moyens automatisés: (a) procéder à l'ingénierie inverse, modifier,

créer des travaux dérivés à partir , décompiler ou extraire le code de la plateforme de services; (b) envoyer, stocker ou transmettre des virus ou d'autres codes informatiques nuisibles via ou sur la plateforme de services; (c) obtenir ou tenter d'obtenir un accès non autorisé à la plate-forme ou aux systèmes de services; (d) interférer avec ou perturber l'intégrité ou la performance de la plate-forme de services; (e) créer des comptes pour la plate-forme de services par des moyens non autorisés ou automatisés; (f) collecter les informations de ou sur les autres utilisateurs de manière non autorisée ou non autorisée; (g) vendre, revendre, louer ou facturer la plateforme de services; ou (h) distribuer ou rendre la plate-forme de services disponible sur un réseau où elle pourrait être utilisée simultanément par plusieurs appareils;

- (h) que le client est responsable de la tenue du client « Services de Compte sûr et sécurisé, et le Client avisera ID-TRACKING sans délai de toute utilisation non autorisée ou violation de la sécurité du client » Compte ou la plate-forme de services ;
- (i) que ID-TRACKING accorde au client une licence d'utilisation de la plate-forme de services limitée, révocable, non exclusive, non sous-licenciable et non transférable. Cette licence a pour seul but de permettre au Client d'utiliser la plate-forme de services, de la manière autorisée par le présent APD. Aucune licence ou droits ne sont concédée au client par implication ou autrement, à l'exception des licences et des droits expressément concédés au client.

6. Mesures techniques et organisationnelles

6.1. ID-TRACKING prendra les mesures techniques et organisationnelles appropriées pour protéger adéquatement les données personnelles contre la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des données personnelles, décrites à l'annexe 1. Ces mesures incluent, mais ne se limitent pas à mesures, et mesures organisationnelles pour :

- (a) la prévention de l'accès des personnes non autorisées aux systèmes de traitement de données à caractère personnel (contrôle d'accès physique),
- (b) empêcher l'utilisation sans autorisation des systèmes de traitement de données à caractère personnel (contrôle d'accès logique),
- (c) veiller à ce que les personnes autorisées à utiliser un système de traitement de données à caractère personnel aient accès uniquement aux données à caractère personnel auxquelles elles ont le droit d'accéder conformément à leurs droits d'accès, et à ce que, au cours du traitement ou de l'utilisation, et après leur stockage, les données à caractère personnel ne puissent être lues, copié, modifié ou supprimé sans autorisation (contrôle d'accès aux données),
- (d) en veillant à ce que les données personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation au cours de la transmission, du transport ou du stockage électroniques, et que les entités cibles pour tout transfert de données à caractère personnel au moyen d'installations de transmission de données puissent être établies et vérifiées (contrôle des transferts),
- (e) en veillant à la mise en place d'une piste d'audit permettant de documenter si et par qui les données personnelles ont été saisies, modifiées ou supprimées des systèmes de traitement des données personnelles (contrôle de la saisie),
- (F) veiller à ce que les données personnelles soient protégées contre la destruction ou la perte accidentelles (contrôle de la disponibilité).

6.2. Les mesures techniques et organisationnelles sont sujettes au progrès technique et au développement ultérieur. À cet égard, ID-TRACKING peut mettre en œuvre une autre mesure adéquate, toutefois, le niveau de sécurité des mesures définies ne doit jamais être réduit. Les changements majeurs doivent être documentés.

7. Sous-traitants

7.1. Le client accepte que ID-TRACKING puisse engager un membre de ID-TRACKING ou des tiers pour traiter des données à caractère personnel afin d'aider ID-TRACKING à fournir les services pour le compte du client (« **sous - traitants** »). ID-TRACKING a ou va conclure un accord écrit avec chaque sous-traitant contenant Les obligations en matière de protection des données ne sont pas moins protectrices que celles de la présente APD dans la mesure applicable à la nature des services fournis par ce sous-traitant. Si le sous-traitant traite les services en dehors de l'UE / EEE, ID-TRACKING veille à ce que le transfert soit effectué conformément aux clauses contractuelles types approuvées par la Commission européenne pour le transfert de données à caractère personnel que le client autorise ID-TRACKING à conclure en son nom, ou que d'autres mécanismes de transfert de données légaux appropriés sont utilisés.

7.2. Les Sous-traitants actuels pour les Services sont définis sur le site Web de ID-TRACKING (« Liste des Sous-traitants ») et le Client accepte et approuve le fait que ID-TRACKING a engagé de tels Sous-traitants pour traiter les données à caractère personnel comme indiqué dans la liste. ID-TRACKING doit notifier un nouveau sous-traitant avant d'autoriser tout nouveau sous-traitant à traiter des données à caractère personnel dans le cadre de la fourniture du service applicable.

7.3. ID-TRACKING avise le trente client (30) jours à l'avance de tout projet de modification concernant l'ajout ou le remplacement d'un Sous-traitants, période pendant laquelle le client peut soulever des objections au processeur sous-nomination. Toute objection doit être soulevée rapidement (et en tout état de cause au plus tard quatorze (14) jours après la notification par ID-TRACKING des modifications envisagées). Si ID-TRACKING choisit de conserver le Sous-traitant opposé, elle en informera le client au moins quatorze

(14) jours avant d'autoriser le sous-traitant à traiter des données personnelles, puis le client peut cesser immédiatement d'utiliser la partie pertinente des services et peut mettre fin à la partie pertinente des services.

7.4. Pour éviter tout doute, si un sous-traitant ne remplit pas ses obligations en vertu d'un accord de Sous-traitants ou en vertu de la loi en vigueur, ID-TRACKING restera entièrement responsable envers le client pour l'exécution de ses obligations en vertu du présent APD.

8. Audit

8.1. Afin de confirmer le respect de cet APD, le client est libre de procéder à un audit en désignant un tiers indépendant qui est tenu de respecter la confidentialité à cet égard. Tout audit de ce type doit avoir lieu pendant les heures normales de bureau de ID-TRACKING et ne sera autorisé que dans la mesure requise par le client pour évaluer sa conformité avec le présent APD. Dans le cadre de cet audit, le client veillera à ce que l'auditeur : (a) examine toutes les informations contenues dans les locaux de ID-TRACKING ;

(b) respecter l'accès raisonnable sur le site et les autres restrictions raisonnablement imposées par ID-TRACKING ; (c) se conformer aux « politiques et procédures de et (d) n'entraverait gravement ID-TRACKING des activités commerciales de l'art. ID-TRACKING se réserve le droit de restreindre ou de suspendre tout audit en cas de non-respect des conditions spécifiées dans la présente section 8.

- 8.2. Dans le cas où le client, un organisme de réglementation ou une autorité de protection des données aurait besoin d'informations supplémentaires ou d'un audit lié aux services, ID-TRACKING s'engage à soumettre ses installations de traitement de données, ses fichiers de données et la documentation nécessaire au traitement des données à caractère personnel par le client. (ou tout tiers, tel que des agents d'inspection ou des auditeurs, sélectionnés par le client) pour vérifier la conformité à la présente APD, sous réserve de notification et de la conclusion par l'auditeur d'un accord de non-divulgence directement avec ID-TRACKING. ID-TRACKING s'engage à fournir au client une coopération raisonnable dans le cadre de telles opérations, notamment en fournissant toutes les informations pertinentes et l'accès à tous les équipements, logiciels, données, fichiers, systèmes d'informations, etc. utilisés pour l'exécution des services, y compris le traitement des données à caractère personnel. Ces audits sont à la charge du client .
- 8.3. L'audit ne peut être entrepris que s'il existe des motifs spécifiques de suspecter une utilisation abusive des données à caractère personnel et au plus tôt deux semaines après que le client a envoyé une notification écrite à ID-TRACKING.
- 8.4. Les constatations relatives à l'audit effectué seront discutées et évaluées par les parties et, le cas échéant, mises en œuvre en conséquence, selon le cas, par l'une des parties ou conjointement par les deux parties. Les coûts de l'audit seront à la charge du client.

9. Notification d'une violation de données

- 9.1. Si ID-TRACKING est informée d'une violation de la sécurité entraînant la destruction accidentelle, non autorisée ou illicite, la divulgation ou l'accès non autorisé à des données à caractère personnel, ID-TRACKING en informera au mieux le client dans les meilleurs délais, après que le Client décide d'informer ou non les personnes concernées et / ou l'autorité de réglementation compétente. Cette obligation de signaler s'applique indépendamment de l'impact de la fuite. ID-TRACKING s'efforcera que les informations fournies soient complètes, correctes et exactes.
- 9.2. Si la loi et / ou les réglementations l'exigent, ID-TRACKING coopérera pour informer les autorités compétentes et / ou les personnes concernées par les données. Le client reste responsable des obligations légales qui en découlent.
- 9.3 L'obligation de signaler inclut en tout état de cause l'obligation de signaler le fait qu'une fuite s'est produite, y compris des détails concernant :

La cause (présumée) de la fuite ;

Les conséquences (actuellement connues et / ou prévues) de celles-ci ; la solution (proposée) ;

Les mesures qui ont déjà été prises.

10. Suppression et retour des données personnelles

- 10.1. Les parties conviennent que, à la fin de la fourniture des services de traitement de données, ID-TRACKING et ses sous-traitants renvoient au choix du client toutes les données à caractère personnel transférées et leurs copies au client ou détruisent toutes les données à caractère personnel. et certifie au client qu'il l'a fait, à moins que la législation imposée à ID-TRACKING ne l'empêche de renvoyer ou de détruire tout ou partie des données personnelles transférées. Dans ce cas, ID-TRACKING garantit qu'elle garantira la confidentialité des données personnelles transférées et ne traitera pas activement les données personnelles transférées. plus. ID-TRACKING et ses sous-traitants garantissent qu'à la demande du client et / ou de l'autorité de surveillance, elle soumettra ses installations de traitement de données à un audit des mesures visées à la section 8.

11 Loi applicable / Forum

11.1. Cet APD est régi et interprété conformément aux lois de la Lituanie.

11.2 Toute réclamation, contestation ou controverse découlant de, découlant de ou liée à cet APD, violation, résiliation ou validité de celle-ci, qui n'a pas été résolue par des négociations de bonne foi entre ID-TRACKING et le client dans un délai de trente (30) Les jours civils suivant la réception d'une notification d'une partie à l'autre demandant des négociations sont réglés par un arbitrage final et obligatoire devant la Cour d'arbitrage commercial de Vilnius, conformément à son règlement d'arbitrage en vigueur à la date de la APD. Les différends seront réglés par un seul arbitre. Une procédure d'arbitrage aura lieu à Vilnius, en Lituanie. Le lieu de l'arbitrage sera Vilnius, en Lituanie. La langue de l'arbitrage sera l'anglais. Les documents pertinents dans d'autres langues seront traduits en anglais si les arbitres le demandent. Tous les frais et dépens des arbitres et de l'arbitrage seront partagés de manière égale, sauf que ID-TRACKING et le Client assumeront les frais de leur propre poursuite et défense, y compris sans les frais d'avocat et la production de témoins. et d'autres preuves. Toute sentence rendue dans le cadre de cet arbitrage est finale et peut être exécutée par l'une ou l'autre des parties.

11.3 Les parties conviennent de garder tous les détails de la procédure d'arbitrage et de la sentence arbitrale strictement confidentiels et doivent déployer tous les efforts raisonnables pour prendre les mesures appropriées pour empêcher la divulgation non autorisée de la procédure, de toute information divulguée à ce sujet et de la sentence rendue.

Description des mesures techniques et organisationnelles mises en place par ID-TRACKING :

ID-TRACKING met en œuvre les mesures décrites dans la présente annexe, à condition que les mesures contribuent directement ou indirectement, peuvent contribuer à la protection des données personnelles pendant la période des services de ID-TRACKING rendu au client. Si ID-TRACKING estime qu'une mesure n'est pas nécessaire pour le service concerné ou une partie de celle-ci, elle la justifiera et conclura un accord avec le client.

Les mesures techniques et organisationnelles sont sujettes au progrès technique et au développement. À cet égard, ID-TRACKING est autorisée à mettre en œuvre d'autres mesures adéquates. Le niveau de sécurité doit correspondre aux meilleures pratiques de l'industrie en matière de sécurité et au moins aux mesures décrites dans les présentes. Tous les changements majeurs doivent être convenus avec le client et documentés.

1. Gestion des risques

1.1. Gestion des risques de sécurité

1. ID-TRACKING doit identifier et évaluer les risques de sécurité liés à la confidentialité, à l'intégrité et à la disponibilité et mettre en œuvre, sur la base de cette évaluation, les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié.
2. ID-TRACKING doit disposer de processus et de procédures documentés pour gérer les risques dans le cadre de ses opérations.
3. ID-TRACKING évaluera périodiquement les risques liés aux systèmes d'information et au traitement, au stockage et à la transmission des informations.

1.2. Gestion des risques de sécurité pour les données personnelles

- 1.2.1. ID-TRACKING doit identifier et évaluer les risques de sécurité liés à la confidentialité, à l'intégrité et à la disponibilité et mettre en œuvre, sur la base de cette évaluation, les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque associé au type de données à caractère personnel et aux finalités traitées par le fournisseur. Société, y compris notamment selon le cas :

- La pseudonymisation et le cryptage des données personnelles ;
- La capacité à garantir la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et des services de traitement ;
- La possibilité de rétablir la disponibilité et l'accès aux données du client en temps utile en cas d'incident physique ou technique ;
- Un processus permettant de tester, d'évaluer et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du traitement.

- 1.2.2. ID-TRACKING doit disposer de processus et de routines documentés pour gérer les risques lors du traitement de Données à caractère personnel pour le compte du Client.
- 1.2.3. ID-TRACKING évaluera périodiquement les risques liés aux systèmes d'information et au traitement, au stockage et à la transmission des données personnelles.

1.3. Politiques de sécurité de l'information

- 1.3.1. ID-TRACKING doit disposer d'un système de gestion de la sécurité de l'information défini et documenté, y compris une politique et des procédures de sécurité de l'information, qui doivent être approuvées par la direction de ID-TRACKING. Ils doivent être publiés au sein de l'organisation de ID-TRACKING et communiqués au personnel compétent de celle-ci.
- 1.3.2. ID-TRACKING examinera périodiquement les politiques et procédures de sécurité de ID-TRACKING et les mettra à jour si nécessaire pour garantir leur conformité à la présente annexe.

2. Organisation de la sécurité de l'information

- ID-TRACKING doit avoir défini et documenté les rôles et responsabilités en matière de sécurité au sein de son organisation.
- ID-TRACKING doit nommer au moins un responsable de la protection des données disposant des compétences appropriées en matière de sécurité et de la responsabilité générale de la mise en œuvre des mesures de sécurité au titre du présent contrat.

Annexe et qui sera la personne de contact du personnel de sécurité du Client.

3. Sécurité des ressources humaines

- ID-TRACKING veille à ce que son personnel traite les informations conformément au niveau de confidentialité requis par la APD.
- ID-TRACKING veille à ce que son personnel concerné soit informé de l'utilisation approuvée (y compris, le cas échéant, des restrictions d'utilisation) des informations, des installations et des systèmes en vertu de la APD.
- ID-TRACKING veille à ce que tout membre du personnel de ID-TRACKING qui exécute des missions en vertu du Contrat soit digne de confiance, réponde aux critères de sécurité établis et a été soumis à une vérification préalable et à une vérification des antécédents pendant toute la durée de la mission.
- ID-TRACKING doit s'assurer que le personnel de ID-TRACKING ayant des responsabilités en matière de sécurité est correctement formé pour effectuer les tâches liées à la sécurité.
- ID-TRACKING fournira ou assurera une formation périodique de sensibilisation à la sécurité au personnel de ID-TRACKING concerné. Cette formation comprendra notamment :
 - (a) Comment gérer la sécurité des informations des clients (c'est-à-dire la protection de la confidentialité, de l'intégrité et de la disponibilité des informations);

- (b) Pourquoi la sécurité de l'information est-elle nécessaire pour protéger les informations et les systèmes des clients ?
- (c) Les types courants de menaces à la sécurité (telles que le vol d'identité, les logiciels malveillants, le piratage, la fuite d'informations et la menace interne);
- (d) L'importance de se conformer aux politiques de sécurité de l'information et d'appliquer les normes / procédures associées ;
- (e) La responsabilité personnelle pour la sécurité de l'information (tels que la protection des renseignements concernant la PI de confidentialité de la clientèle et signalement des violations de données effectives et présumées).

4 Contrôle d'accès

ID-TRACKING doit avoir une politique de contrôle d'accès définie et documentée pour les installations, sites, réseaux, systèmes, applications et accès aux informations / données (y compris les contrôles d'accès physique, logique et à distance), un processus d'autorisation pour l'accès et les privilèges des utilisateurs, des procédures de révocation d'accès droits et une utilisation acceptable des privilèges d'accès pour le personnel de ID-TRACKING.

ID-TRACKING doit mettre en place un processus officiel et documenté d'enregistrement et de désenregistrement des utilisateurs pour permettre l'attribution de droits d'accès.

ID-TRACKING attribuera tous les privilèges d'accès sur la base du principe du besoin de savoir et du principe du moindre privilège.

ID-TRACKING utilisera une authentification forte (multi-facteurs) pour les utilisateurs d'accès distant et les utilisateurs se connectant à partir d'un réseau non sécurisé.

ID-TRACKING doit s'assurer que son personnel dispose d'un identifiant personnel et unique (ID utilisateur) et utilise une technique d'authentification appropriée, qui confirme et garantit l'identité des utilisateurs.

5 Sécurité physique et environnementale

ID-TRACKING doit protéger les installations de traitement de l'information contre les menaces et les dangers externes et environnementaux, y compris les pannes d'alimentation / de câblage et autres perturbations causées par des défaillances des services publics. Cela inclut le périmètre physique et la protection d'accès.

6 Sécurité des opérations

ID-TRACKING doit mettre en place un système de gestion des modifications afin d'apporter des modifications aux processus opérationnels, aux installations et aux systèmes de traitement de l'information. Le système de gestion des modifications doit inclure des tests et des révisions avant la mise en œuvre des modifications, telles que des procédures pour traiter les modifications urgentes, des procédures de restauration pour récupérer des modifications ayant échoué, des journaux indiquant ce qui a été modifié, quand et par qui.

ID-TRACKING mettra en œuvre une protection contre les logiciels malveillants afin de garantir que tout logiciel utilisé pour la fourniture des Services au Client par ID-TRACKING est protégé contre les logiciels malveillants.

ID-TRACKING fera des copies de sauvegarde des informations critiques et en testera des copies de sauvegarde pour s'assurer que les informations peuvent être restaurées comme convenu avec le client.

ID-TRACKING enregistre et surveille les activités, telles que la création, la lecture, la copie, la modification et la suppression des données traitées, ainsi que les exceptions, les défaillances et les événements liés à la sécurité des informations, et les examine régulièrement. En outre, ID-TRACKING protégera et stockera (pendant au moins 6 mois ou toute période définie par la loi sur la protection des données) les informations du journal et, sur demande, transmettra les données de surveillance au client. Les anomalies / incidents / indicateurs de compromission doivent être signalés conformément aux exigences en matière de gestion des atteintes à la sécurité des données énoncées à la clause 9 ci-dessous.

ID-TRACKING gèrera les vulnérabilités de toutes les technologies pertinentes telles que les systèmes d'exploitation, les bases de données et les applications de manière proactive et rapide.

ID-TRACKING doit établir des lignes de base de sécurité (renforcement) pour toutes les technologies pertinentes telles que les systèmes d'exploitation, les bases de données et les applications.

ID-TRACKING doit s'assurer que le développement est séparé de l'environnement de test et de production.

7. Sécurité des communications

ID-TRACKING doit mettre en œuvre des contrôles de sécurité du réseau tels que le niveau de service, le pare-feu et la séparation pour protéger les systèmes d'information.

8 Relation avec les sous-traitants

ID-TRACKING doit refléter le contenu de cette annexe dans ses accords avec les sous-traitants qui exécutent les tâches assignées dans le cadre de la APD.

ID-TRACKING surveille régulièrement, l'examen et vérifier la conformité de processeur Sous cette annexe.

À la demande du client, ID-TRACKING fournira au client des preuves de la conformité du sous-traitant à la présente annexe.

9 Gestion des violations de données

ID-TRACKING doit avoir établi des procédures pour la gestion des violations de données.

ID-TRACKING informera le client de toute violation de données (y compris, mais sans s'y limiter, les incidents liés au traitement de données à caractère personnel) dès que possible mais au plus tard dans les 36 heures après que la violation de données a été identifiée.

Tous les rapports d'incidents liés à la sécurité doivent être traités comme des informations confidentielles et cryptés à l'aide de méthodes de cryptage standard.

Le rapport de violation de données doit contenir au moins les informations suivantes :

- (a) La nature de la violation de données,
- (b) La nature des données personnelles concernées,
- (c) Les catégories et le nombre de personnes concernées,
- (d) Le nombre d'enregistrements de données à caractère personnel concernés,
- (e) Mesures prises pour remédier à la violation de données,
- (f) Les conséquences possibles et les conséquences néfastes de la violation de données, et
- (g) Toute autre information que le client est tenu de communiquer à l'autorité de contrôle ou à la personne concernée.

En vertu de la présente clause 9, ID-TRACKING peut, dans la mesure où cela est juridiquement possible, réclamer une indemnité pour services de support qui ne peut être attribuée à une défaillance de ID-TRACKING.

10. Gestion de la continuité des opérations

ID-TRACKING doit identifier les risques de continuité des activités et prendre les mesures nécessaires pour contrôler et atténuer ces risques.

ID-TRACKING doit disposer de processus et de procédures documentés pour gérer la continuité des activités.

ID-TRACKING veille à ce que la sécurité de l'information soit intégrée aux plans de continuité des opérations.

ID-TRACKING évaluera périodiquement l'efficacité de sa gestion de la continuité des activités et sa conformité aux exigences de disponibilité (le cas échéant).