Programme de Protection des Données des Abonnés d'Alida
En vigueur au 1er janvier 2022

La société du groupe Alida qui a conclu un contrat avec l'Abonné ("**Alida**" ou "**nous**") est au service de l'Abonné et protège les données de l'Abonné conformément aux termes de la présente Annexe relative au Traitement des Données ("**l'Annexe**").

1. Définitions

A. "**Contrat**" désigne le contrat conclu entre Alida et l'Abonné aux termes duquel Alida convient de mettre la Solution à la disposition de l'Abonné, ainsi que toutes les fiches techniques, spécifications de service et autres documents techniques, ainsi que leurs modifications successives, qui peuvent y être incorporées par référence.

B. "**Sauvegarde**" désigne une copie supplémentaire des données à utiliser si la copie originale est endommagée ou indisponible. La copie supplémentaire des données est conservée séparément de la copie originale.

C. "**Membre**" désigne une personne physique dont les données sont traitées dans la Solution, y compris lorsqu'elle est invitée par ou au nom de l'Abonné à consulter, soumettre, visualiser ou commenter les Données de l'Abonné sur le Site Web et/ou à participer à tout forum, discussion, recherche, enquête/sondage, étude ou tout autre moyen ou forme de collecte de données administré(e) par la Solution.

D. "**Test d'Intrusion**" désigne une recherche informatique de mauvaises configurations et de Défauts de Sécurité par un expert en sécurité sans accès au code source du système ;

E. "**Données à caractère personnel**" désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une « personne physique identifiable » une personne physique 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 éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

F. "**Système de Production**" et "**Réseau de Production**" désigne un environnement informatique utilisé pour héberger la Solution et sujet à des contrôles d'accès et à des procédures de gestion régissant la réalisation de changements ;

G. "**Violation de Sécurité**" désigne tout accès, utilisation ou divulgation non autorisé(e) et confirmé(e) des Données de l'Abonné ;

H. "**Défaut de Sécurité**" désigne une défaillance technique du logiciel ou du matériel qui, si elle est exploitée, pourrait entraîner un accès non autorisé à la Solution ou aux Données de l'Abonné ;

I. "**Questionnaire de Sécurité**" désigne tout formulaire élaboré par l'Abonné ou lui appartenant, ou tout autre moyen permettant de recueillir des informations sur les fonctionnalités d'Alida en matière de sécurité, de confidentialité ou de protection des données ;

J. "**Analyse de Sécurité**" désigne une recherche automatisée de Défauts de Sécurité dans un système sans accès au code source de ce système ;

K. "**Solution**" désigne la plate-forme technologique et les services automatisés appartenant à Alida, y compris toutes les mises à niveau et mises à jour standard, mais excluant tous les produits ou logiciels de tiers qui peuvent interagir avec la plate-forme technologique d'Alida ;

L. "**Abonné**" désigne un client d'Alida qui a conclu un contrat d'abonnement avec Alida pour accéder à la Solution et l'utiliser, en ce compris les utilisateurs de la Solution tels qu'autorisés par l'Abonné ;

M. "**Données de l'Abonné**" désigne les informations téléchargées ou collectées via la Solution par l'Abonné, ou soumises à la Solution par les Membres ;

N. "**Sous-traitant ultérieur**" désigne une partie fournissant des services à Alida et contribuant ainsi à la mise à disposition de la Solution. Un Sous-traitant ultérieur peut avoir accès aux Données de l'Abonné ; et

O. "**Fournisseur**" désigne une partie fournissant des services à Alida et contribuant ainsi à la mise à disposition de la Solution, sans toutefois accéder aux Données de l'Abonné lors de l'exécution des dits services ;

P. "**Site Web**" désigne le système d'exploitation en ligne de la Solution identifié par l'Abonné, accessible via un domaine appartenant à cet Abonné.

2. Contrôle et Propriété

Les Abonnés possèdent et contrôlent toutes leurs Données de l'Abonné. Alida n'utilise pas les Données de l'Abonné, sauf : (a) dans l'intérêt et pour le compte de l'Abonné ; (b) lorsque cela est nécessaire pour fournir les Services ; ou (c) comme prévu ou prescrit par le Contrat. Alida conserve tous les droits sur la Solution, la technologie d'Alida et les données d'Alida, y compris toute information qu'Alida découvre, crée ou obtient en fournissant la Solution, à l'exception des Données de l'Abonné.

3. Sécurité

Alida applique des mesures techniques, administratives et organisationnelles de sécurité des données qui répondent à ou dépassent les exigences prévues dans la description des Mesures Techniques et Organisationnelles d'Alida (ci-jointe). Alida peut mettre à jour et modifier périodiquement le document précité, à condition qu'Alida ne réduise pas le niveau de sécurité fourni en vertu de celui-ci, sauf avec le consentement de l'Abonné ou avec un préavis écrit de 90 jours.

4. Assistance en matière d'Obligations de Conformité

A la demande raisonnable de l'Abonné, Alida (a) assistera raisonnablement l'Abonné en ce qui concerne l'accès aux données, la suppression, la portabilité et autres demandes, sous réserve d'une indemnisation pour tout service personnalisé demandé à Alida, et (b) conclura des accords contractuels supplémentaires pour répondre à des exigences spécifiques qui sont imposées à l'Abonné en vertu de lois impératives concernant les Données de l'Abonné et qui, en raison de leur nature, ne peuvent être satisfaites que par Alida dans son rôle de fournisseur de services ou que l'Abonné explique et confie spécifiquement à Alida dans un addendum ou un avenant au Contrat applicable, sous réserve du remboursement de coûts ou de frais supplémentaires, selon les cas. Lorsque l'Abonné est situé dans l'EEE ou au Royaume-Uni et qu'il contracte avec une société du groupe Alida qui n'est pas située dans l'EEE ni dans un « pays tiers adéquat » (tel que déterminé par la Commission européenne), Alida acceptera les Clauses Contractuelles Types de la Commission européenne et l'Addendum International de Transfert de Données du Royaume-Uni pour les transferts transfrontaliers. Si l'Abonné ne peut plus utiliser licitement les produits d'Alida en raison de changements dans la loi ou de modifications technologiques, Alida permettra à l'Abonné de résilier certains ou tous les contrats et fournira une aide à la transition ou à la migration telle que raisonnablement demandée, sujet à des frais de résiliation et autres frais d'intervention d'Alida tels que mutuellement convenus de bonne foi par les parties.

5. Violations de Sécurité

Dans le cas d'une Violation de Sécurité, Alida fera des efforts commercialement raisonnables pour : (i) limiter et atténuer son impact dans les meilleurs délais ; (ii) mener une enquête pour déterminer la cause de la Violation de Sécurité ; (iii) notifier l'Abonné de la Violation de Sécurité dans les meilleurs

délais ; et (iv) fournir les informations raisonnablement demandées par l'Abonné afin de l'aider à s'acquitter de ses propres obligations légales. Il est précisé que la divulgation du contenu d'un Site Web par un internaute (ayant répondu à un questionnaire et autorisé à accéder à ce Site Web) ne constitue pas une Violation de Sécurité.

6. Audit

Chaque année et à ses frais, Alida fera réaliser un audit indépendant de ses capacités de sécurité et de confidentialité par un professionnel qualifié choisi par Alida. Sur demande écrite, Alida fournira à l'Abonnée le rapport d'audit ("**Rapport d'Audit**"). Sur demande écrite de l'Abonné, Alida fournira également un calendrier commercialement raisonnable pour corriger tout défaut important relatifs aux contrôles de sécurité et de confidentialité d'Alida identifiés dans le Rapport d'Audit ("**Défaut Important Identifié**"). Alida permettra à l'Abonné ou à l'auditeur désigné par celui-ci d'effectuer son propre audit des contrôles de confidentialité et de sécurité d'Alida ("**Audit de l'Abonné**") seulement dans les circonstances suivantes : (i) le Rapport d'Audit n'est pas disponible et Alida ne peut fournir un calendrier commercialement raisonnable quant au moment où il sera mis à la disposition de l'Abonné ; et (ii) le Rapport d'Audit présente des Défauts Importants Identifiés pour lesquels Alida n'a pas fourni /de calendrier de correction. Tout Audit de l'Abonné aura lieu : (i) aux seuls frais de l'Abonné ; (ii) pendant les heures normales d'ouverture d'Alida et pour une durée qui ne pourra excéder 2 jours ouvrables ; (iii) en le sollicitant par écrit auprès d'Alida au moins 10 jours ouvrables à l'avance, cette demande devant inclure une présentation claire de la portée de l'audit et toute preuve ou autre ressource que l'Abonné souhaite examiner ; (iv) avec le consentement écrit d'Alida, qui ne doit pas être indûment refusé ou retardé ; (v) conformément aux accords de confidentialité appropriés ; et (vi) seulement une fois par année contractuelle d'abonnement. Il est précisé que toute demande de l'Abonné pour remplir un Questionnaire de Sécurité sera considérée comme une demande de droits d'audit, qu'Alida peut honorer en fournissant un Rapport d'Audit. Alida peut également, à sa seule discrétion, fournir l'un des documents suivants à titre de réponse au Questionnaire de Sécurité de l'Abonné : (i) un questionnaire sur la Collecte d'Informations Standard SIG (*Standard Information Gathering*) dûment rempli fourni par *Shared Assessments* et le *Santa Fe Group* ; (ii) un questionnaire dument rempli fourni par la *Cloud Security Alliance* (CSA); ou (iii) un autre questionnaire standard sensiblement équivalent.

7. Sites d'hébergements

Les systèmes principaux d'Alida, et le stockage de données associé, sont hébergés dans une infrastructure d'hébergement au sein de l'un des sites suivants : (i) Les Données des Abonnés établis sur le continent américain sont hébergées dans les régions au sein desquelles Amazon Web Services est disponible aux États-Unis ou au Canada ; (ii) les Données des Abonnés situés en Europe, au Moyen-Orient ou en Afrique sont hébergées dans la région au sein de laquelle Amazon Web Services est disponible en Allemagne ; et (iii) les Données des Abonnés situés en Asie-Pacifique sont hébergées dans la région au sein de laquelle Amazon Web Services est disponible à Singapour. Alida peut relocaliser ses infrastructures d'hébergement et toutes les Données des Abonnés qui s'y trouvent à condition que cette relocalisation : (i) soit publiée sur le site web d'Alida au moins 60 jours à l'avance ; et (ii) qu'Alida conserve les Données des Abonnés dans la même région géographique pertinente qui est l'une des suivantes : (a) l'Amérique du Nord pour les abonnés situés sur le continent américain ; (b) l'Union européenne pour les abonnés situés en Europe, au Moyen-Orient ou en Afrique ; ou (c) la région Asie-Pacifique pour les abonnés situés en Océanie, Asie du Sud-Est, Asie du Sud et Asie de l'Est. Alida tient à jour une liste des infrastructures d'hébergement à l'adresse suivante : https://www.alida.com/trust/legal/ ou à toute autre page de son site web ayant le même objet ("**Page de Notifications aux Abonnés**"). Il est précisé qu'entre Alida et l'Abonné, il est de la responsabilité de l'Abonné de se conformer à toute réglementation qui exige l'hébergement des Données de l'Abonné dans une région spécifique. Alida conserve un répertoire global d'utilisateurs pour gérer l'authentification du compte administrateur de l'Abonné et son routage vers la région d'hébergement pertinente, comme cela est décrit ci-dessus. Les données contenues dans ce répertoire d'utilisateurs sont hébergées au Canada.

8. Fournisseurs et Sous-traitants Ultérieurs

Alida s'engage à maintenir des contrats adéquats avec tous les Fournisseurs et Sous-traitants Ultérieurs afin d'assurer la conformité avec les obligations figurant dans cette Annexe et sera responsable de la conformité de ses Fournisseurs et Sous-traitants Ultérieurs avec les stipulations de la présente Annexe. Alida s'engage à tenir une liste à jour des Fournisseurs et Sous-traitants Ultérieurs et de leurs localisations sur sa Page de Notification aux Abonnés. Les abonnés peuvent s'inscrire pour recevoir des notifications automatiques des mises à jour de la liste des Fournisseurs et des Sous-traitants Ultérieurs.

9. Suppression et Anonymisation

Lors de la résiliation du Contrat, Alida accordera à l'Abonné un délai de 30 jours afin d'exporter les Données de l'Abonné depuis la Solution. A l'issue de cette période de 30 jours, Alida n'aura aucune obligation de les conserver et supprimera de manière définitive toutes les Données de l'Abonné stockées dans la Solution. Les Sauvegardes des Données de l'Abonné seront supprimées ou écrasées de façon sécurisée 90 jours plus tard.
Sur demande et si cela est possible, Alida permettra à l'Abonné de désigner des champs spécifiques au sein d'un questionnaire comme étant des Données à caractère personnel devant être écrasées après expiration du délai spécifié par l'Abonné. Seuls les champs associés aux Membres dont le compte a été déclaré inactif seront écrasés après expiration du délai spécifié par l'Abonné. Il est précisé à toutes fins utiles que la fiche du Membre sera considérée comme anonymisée par la Solution lorsque les champs spécifiés par l'Abonné seront écrasés de telle sorte qu'ils ne contiennent plus de données d'identification ; en outre, la Solution écrasera l'adresse électronique, l'identifiant, le nom et le numéro de téléphone du Membre. Une fois écrasées, les données initiales sont ensuite conservées à titre de Sauvegarde pendant 90 jours.
Nonobstant ce qui précède, Alida ne purge pas les données des journaux (*logs*) de sécurité et de performance à la fin de l'Abonnement, de telles données étant par la suite écrasées du système central de logs d'Alida au fil du temps. Les journaux (*logs*) ne contiennent généralement pas de données fournies par un Membre, bien qu'ils puissent contenir l'adresse électronique et l'adresse IP, et d'autres informations d'identification dans certains cas.

10. Aucune vente ni partage d'informations pour la Publicité Comportementale Ciblée (*Cross context behavioral advertising*)

Alida n'accepte ni ne divulgue aucune Donnée de l'Abonné en contrepartie de paiements, services ou autres éléments de valeur. Alida ne vend ni ne partage aucune Donnée de l'Abonné, étant précisé que les termes « vendre » et « partager » s'entendent au sens que leur donne le *California Consumer Privacy Act* de 2018, tel que modifié, notamment par le *California Privacy Rights Act* (« CCPA »). Alida traite les Données de l'Abonné uniquement aux fins commerciales spécifiées dans le Contrat. Alida ne conserve pas, n'utilise pas et ne divulgue pas les Données de l'Abonné (a) pour la publicité comportementale ciblée, ou (b) en dehors de la relation commerciale directe avec l'Abonné. Alida ne croise pas les Données de l'Abonné avec d'autres données dès lors que cela serait incompatible avec les limitations imposées aux fournisseurs de services en vertu du CCPA.

11. Données à caractère personnel dans les pays de l'EEE

En ce qui concerne les Données de l'Abonné qui sont soumises au Règlement Général sur la Protection des Données de l'UE (RGPD) ou à des lois similaires d'autres pays en tant que "données à caractère personnel", Alida accepte les obligations suivantes en qualité d'importateur de données, de sous-traitant ou de sous-traitant ultérieur de l'Abonné et garantit qu'Alida :

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis ; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
c) prend toutes les mesures requises en vertu de l'article 32 du RGPD (sécurité du traitement) ;
d) respecte les conditions visées aux paragraphes 2 et 4 de l'article 28 du RGPD pour recruter un autre sous-traitant ;
e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III du RGPD, y compris, de manière non limitative, le droit d'accès, de rectification, d'effacement et de portabilité des données à caractère personnel des personnes concernées (afin de dissiper toute ambiguïté, le sous-traitant doit uniquement aider et permettre au responsable du traitement de remplir ses obligations en matière de respect des droits des personnes concernées, mais le sous-traitant ne doit pas répondre directement aux personnes concernée) ;
f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD (sécurité des données à caractère personnel), compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;
g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ; et
h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

12. Notification des Modifications

Périodiquement, Alida peut mettre à jour ses pratiques en matière de sécurité et de confidentialité. Tout changement important sera affiché sur la Page des Notifications aux Abonnés au moins 30 jours avant leur entrée en vigueur, sauf indication contraire dans le Contrat. Dans l'hypothèse où l'Abonné estime que ce(s) changement(s) important(s) n'est (ne sont) pas acceptable(s), l'Abonné peut mettre fin au Contrat le liant à Alida conformément à ses stipulations.

13. Intégration

La présente Annexe engage Alida dans la mesure où elle est expressément convenue ou incorporée par référence dans un Contrat dûment signé. La présente Annexe ne crée pas de droits au bénéfice de tiers. Aucune autre obligation relative aux Données de l'Abonné n'engage Alida, sauf si elle est spécifiquement et expressément convenue par écrit par référence explicite au Contrat et à la présente Annexe.

Description des Mesures Techniques et Organisationnelles mises en place par Alida

1. Généralités

Ce document relatif aux Mesures Techniques et Organisationnelles décrit les processus, l'infrastructure et les politiques qu'Alida a mis en place pour protéger ses systèmes et les Données des Abonnés. Les termes en majuscules utilisés dans le présent document ont la même signification que dans le document « Programme de Protection des Données des Abonnés d'Alida ».

2. Politiques et gouvernance

Alida a mis en place la structure de gouvernance suivante en ce qui concerne ses politiques et normes de sécurité et de confidentialité (les "**Politiques**") :

A. Les Politiques d'Alida ont été approuvées par la direction d'Alida (la "**Direction**") ;

B. Un membre des instances dirigeantes est responsable de la sécurité et de la confidentialité chez Alida et rend compte périodiquement à la Direction et au conseil d'administration d'Alida (le "**Conseil d'Administration**") sur ces questions ;

C. Les risques sont enregistrés de manière centralisée et signalés à la Direction et au Conseil d'Administration le cas échéant ;

D. Alida revoit périodiquement ses Politiques et la documentation qui les accompagne pour en vérifier la pertinence ;

E. La non-conformité à une Politique requiert des approbations conformément à un cadre décisionnel clair ;

F. La non-conformité sans l'approbation autorisée des Politiques a des conséquences pouvant aller jusqu'au licenciement ;

G. Chaque année, Alida mène une formation de sensibilisation à la sécurité et à la confidentialité des utilisateurs ;

H. Tous les collaborateurs paraphent les Politiques chaque année ;

I. Tous les nouveaux collaborateurs d'Alida font l'objet d'une vérification de leurs antécédents judiciaires lorsque la loi le permet ;

J. Tous les salariés sont soumis à des accords de confidentialité écrits.

3. Sécurité des Centres de Données

Alida héberge la Solution dans des centres d'hébergement de données de catégorie « Enterprise Class » qui fournissent :

A. Des rapports d'audit annuels indépendants sur leurs capacités en matière de sécurité et de disponibilité. De tels rapports incluent, sans que cette liste soit limitative : Les rapports d'audit des *Services Organization Controls* ("SOC") de l'AICPA ou les certifications ISO27001 ;

B. Des systèmes de refroidissement redondants, extinction d'incendie, alimentation/énergie et communications ; et

C. Des services de gardiennage 24 heures sur 24 et 7 jours sur 7, un contrôle d'accès physique et une surveillance vidéo.

4. Sécurité des infrastructures

Alida a mis en place les mécanismes de sécurité suivants :

A. La Solution est protégée par des pare feu ou une technologie fonctionnellement équivalente qui restreint le trafic à ce qui est uniquement nécessaire pour fournir le service ;

B. Le trafic réseau dans le réseau hébergeant la Solution est surveillé par détection d'intrusion ;

C. Tous les accès à la Solution et à son infrastructure de soutien sont enregistrés de manière centralisée ;

D. Surveillance automatisée des activités malveillantes 24 heures sur 24 et 7 jours sur 7 ;

E. Des hôtes Bastion et un accès VPN authentifié à deux facteurs au Réseau de Production ; et

F. Des logiciels anti-virus.

5. Environnement multi-tenant

Alida fournit une Solution multi-tenant qui stocke les données de plusieurs Abonnés, et offre les protections suivantes :

A. Chaque Site Web est dédié à un seul Abonné ;

B. Les Sites Web sont identifiés de façon unique par leur nom de domaine et leur identifiant de compte sous-jacent ;

C. L'accès aux Sites Web est uniquement accordé aux identités directement associées au compte de l'Abonné ;

D. Les données sont logiquement séparées en utilisant soit des schémas de base de données distincts, soit des attributs de données qui sont utilisés par le code d'application pour prendre des décisions relatives à l'accès ; et

E. Les journaux d'infrastructure détaillés ne sont pas accessibles aux Abonnés.

6. Sécurité des Applications

Alida assure les contrôles suivants au sein et autour de la Solution :

A. Accès protégé par nom d'utilisateur et mot de passe au portail de l'administrateur et intégration optionnelle avec les Fournisseurs d'Identité SAML 2.0 ;

B. Accès authentifié au Site Web ;

C. Journalisation de la création/suppression/déploiement d'études ainsi que de toutes les créations/modifications/suppressions d'utilisateurs ; et

D. Des pratiques de développement sécurisées et l'utilisation de bibliothèques logicielles sûres. Aux fins de la présente section, une "bibliothèque logicielle sûre" est une bibliothèque fournie par le fabricant qui est exempte de défauts de sécurité connus et qui est conçue de telle sorte que les développeurs sont obligés d'utiliser la bibliothèque d'une manière qui n'introduit pas involontairement des défauts de sécurité dans la Solution.

7. Chiffrement des données

A. Toutes les connexions à la Solution sont protégées à l'aide de canaux chiffrés, y compris, de manière non limitative, par le *Transport Layer Security* (TLS) ;

B. Toutes les Sauvegardes sont chiffrées ; et

C. Tous les systèmes stockant les Données de l'Abonné utilisent un stockage sur disque qui est chiffré durant leur stockage (*at rest*).

8. Fonctionnement

A. Alida a mis en place des processus comprenant des procédures de gestion des vulnérabilités, de réponse aux incidents et de correctifs de sécurité pour se protéger contre les menaces connues et émergentes.

B. Les modifications apportées aux Systèmes de Production ne peuvent être mises en œuvre que par des administrateurs de système autorisés, suivant un processus défini d'assurance qualité, de gestion des modifications et d'approbation.

9. Reprise après Sinistre et Continuité des Activités

A. Alida maintiendra des *snapshots* sur place et une capacité suffisante pour restaurer les Sites Web individuels dans les 48 heures, sans perte de données de plus de 24 heures ;

B. Si Alida envoie des sauvegardes des données hors site, ces sauvegardes seront chiffrées et les clés de chiffrement resteront sous le contrôle d'Alida ; et

C. Dans l'éventualité d'une perte catastrophique d'un centre de données complet, Alida déploiera ses efforts commercialement raisonnables pour récupérer le Site Web de l'Abonné.

10. Politiques de confidentialité et journaux (logs)

A. Alida applique des politiques de confidentialité pour régir ses propres pratiques internes en ce qui concerne le traitement sécurisé et réglementaire des Données à caractère personnel. Ces politiques traitent du consentement, de la limitation de la collecte, de la qualité des données, de la limitation de l'utilisation, de la divulgation, de la conservation, des transferts, des droits des personnes concernées et de la sécurité, comme l'exige la Règlementation Applicable sur la Protection de la vie privée, en ce qui concerne le traitement des Données à caractère personnel. La "**Réglementation Applicable sur la Protection de la vie privée**" comprend, de manière non limitative :

i. Le *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") au Canada ;

ii. Le Règlement Général sur la Protection des Données 2016/679 ("**RGPD**") ;

iii. Le *Federal Privacy Act 1988* en Australie ;

iv. Le *Personal Data Protection Act 2012* à Singapour ; et

v. Le *California Consumer Privacy Act* ("**CCPA**").

B. Alida conservera les journaux (*logs*) contenant des informations personnelles telles que les adresses électroniques et les adresses IP, ainsi que les actions effectuées sur la Solution à des fins de sécurité et de contrôle.

11. Tests de Sécurité

A. Alida effectuera un Test d'Intrusion annuel de la Solution en faisant appel à un fournisseur externe sélectionné à la seule discrétion d'Alida. Une fois que les Défauts de Sécurité identifiés seront corrigés, Alida confirmera cette correction, ou fera en sorte que le même fournisseur externe fournisse une confirmation de celle-ci ;

B. Alida effectuera des Analyses de Sécurité mensuelles de la Solution ;

C. Sur demande de l'Abonné, Alida fournira la preuve que de tels Tests d'Intrusion et Analyses de Sécurité ont été effectués ;

D. Une fois par année contractuelle d'abonnement et avec un préavis d'au moins dix (10) jours ouvrables, l'Abonné ou son représentant pourra effectuer ses propres Tests d'Intrusion sur un Site Web fourni par Alida, et non sur le Site Web de l'Abonné. L'Abonné accepte de renoncer à ce droit si Alida, à sa seule discrétion, fournit un rapport de portée équivalente qui ne date pas de plus de douze (12) mois ;

E. Nonobstant les limitations précédentes relatives à la fréquence des Tests d'Intrusion, les tests supplémentaires visant à confirmer que les problèmes signalés précédemment ont été corrigés ne sont pas limités en fréquence ;

F. À des intervalles convenus d'un commun accord entre les parties, un Abonné ou son représentant pourra effectuer une Analyse de Sécurité de son propre Site Web une fois que sa méthodologie aura été examinée et approuvée par Alida ;

G. Un tel Test d'Intrusion annuel ou Analyse de Sécurité par l'Abonné existe en plus des droits d'audit tels que prévus dans le Programme de Protection des Données des Abonnés d'Alida ;

H. Alida peut raisonnablement refuser d'approuver un Test d'Intrusion ou une Analyse de Sécurité s'il a des raisons de croire que la méthodologie que l'Abonné ou son représentant utilisera perturbe la performance, la disponibilité ou l'intégrité de la Solution ;

I. Si le Test d'Intrusion ou l'Analyse de Sécurité effectués par l'Abonné ou son représentant perturbent la performance, la disponibilité ou l'intégrité de la Solution, Alida peut alors exiger de l'Abonné qu'il les arrête ou les fasse arrêter immédiatement jusqu'à ce qu'Alida ait identifié la raison de la perturbation et la considère résolue ;

J. L'Abonné fournira toutes les informations raisonnablement demandées par Alida sur la nature de ses activités relatives au Test d'Intrusion et à l'Analyse de Sécurité avant de commencer son travail. Ces informations comprennent, de manière non limitative : les adresses IP sources, les coordonnées, les noms des collaborateurs ou des représentants et les horaires des tests ;

K. L'Abonné ou son représentant se conformera aux directives d'Alida concernant l'exécution des Tests d'Intrusion et des Analyses de Sécurité et, en retour, Alida fournira à l'Abonné l'accès nécessaire pour effectuer ces Tests d'Intrusion et Analyses de Sécurité ;

L. Si l'Abonné exige que les Défauts de Sécurité identifiés soient corrigés, l'Abonné ou son représentant doit fournir par écrit les renseignements complets sur ce Défaut de Sécurité afin qu'Alida puisse indépendamment évaluer, reproduire et vérifier l'existence du Défaut de Sécurité ; et

M. Dans les dix (10) jours ouvrables suivant la confirmation par Alida de l'existence des Défauts de Sécurité signalés, Alida fournira, sur demande, un plan de mesures correctives suivant les échéances prévues dans la section suivante.

12. Mesures correctives portant sur des Défauts de Sécurité

A. Alida utilise des techniques de notation standard de l'industrie, telles que le *Common Weakness Scoring System* (CWSS) et le *Common Vulnerability Scoring System* (CVSS), pour évaluer la gravité de tout Défaut de Sécurité identifié. Alida peut, à sa seule discrétion, les remplacer par des techniques de notation équivalentes.

B. Alida évaluera un Défaut de Sécurité en utilisant les techniques susmentionnées et classera les défauts par impact de la manière suivante :

Désignation courante de l'impact	CVSS	CWSS
Critique	9.0 à 10.0	90 à 100
Elevé	7.0 à 8.9	70 à 89
Moyen	4.0 à 6.9	40 à 69
Faible	0.0 à 3.9	0 à 39

C. Alida remédiera aux Défauts de Sécurité contenus dans la Solution selon les délais suivants, décomptés à partir de la confirmation par Alida du Défaut de Sécurité signalé :

Désignation courante de l'impact	Délai
Critique	Rapidement et au maximum quatorze (14) jours
Elevé	Dans les quarante-cinq (45) jours
Moyen	Dans les quatre-vingt-dix (90) jours
Faible	Dans les cent quatre-vingt jours (180) jours

D. Alida peut, à sa convenance, mettre en œuvre une solution temporaire au Défaut de Sécurité afin de respecter les échéances mentionnées ci-dessus. De telles solutions temporaires peuvent consister à désactiver ou modifier temporairement des fonctionnalités spécifiques, tout en travaillant à mettre en œuvre une solution permanente pour corriger le Défaut de Sécurité. Si Alida choisit de désactiver ou de modifier temporairement une fonctionnalité pour remédier au Défaut de Sécurité, l'Abonné ne saurait considérer qu'il s'agit d'une réduction du service ;

E. Alida peut raisonnablement différer la correction d'un Défaut de Sécurité signalé, et de manière non limitative, pour les raisons suivantes :

a. Le Défaut de Sécurité est signalé trop tardivement dans le cycle de la version actuelle pour être intégré en toute sécurité au regard des pratiques d'Alida en matière de gestion des modifications ;
b. Un changement ou un correctif planifié permettra de remédier au Défaut de Sécurité dans un délai raisonnable ; ou
c. Toutes les ressources disponibles sont déjà engagées sur un Défaut de Sécurité d'un impact plus important.

F. Alida peut légitimement refuser t de remédier à un Défaut de Sécurité si ce défaut ne permet pas en pratique d'accéder aux Données de l'Abonné ou à la Solution.