

ACCORD SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

1. OBJET

Le présent Accord sur la protection des données a pour objet de définir les conditions dans lesquelles AutonomieCompta s'engage à effectuer les opérations de Traitement des Données à caractère personnel fournies par l'Abonné/Utilisateur pour l'exécution des Services.

Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter les dispositions de la loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et modifiée (ci-après « Loi Informatique et Libertés ») et du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après le "RGPD").

2. DEFINITIONS

Les définitions attachées au présent Accord sur la protection des données sont disponibles dans l'annexe des définitions.

3. ENTRÉE EN VIGUEUR ET DURÉE

Le présent Accord entre en vigueur à compter de la signature du Contrat auquel il est attaché et reste en vigueur durant toute la durée de la relation contractuelle unissant AutonomieCompta et l'Abonné/Utilisateur.

4. STATUT DES PARTIES

Les Parties sont convenues que l'Utilisateur/Abonné est le « Responsable de traitement » et AutonomieCompta est le "Sous-Traitant" concernant les traitements des Données à caractère personnel qu'elles soient fournies directement ou indirectement à AutonomieCompta par l'Utilisateur/Abonné ou par un Administrateur qui s'est vu accorder par l'Utilisateur/Abonné l'accès aux Services.

AutonomieCompta est autorisée par l'Utilisateur/Abonné à traiter, pour le compte du Responsable de traitement, les Données à

caractère personnel et Données de santé nécessaires à la fourniture des Services pour les finalités et dans le strict respect des conditions mentionnées ci-après.

Il est précisé que l'engagement d'AutonomieCompta se limite à l'installation, la fourniture des Services et l'hébergement de la Plateforme AutonomieCompta.

Dès lors que le Responsable de traitement renseigne des Données à caractère personnel ou Données de santé de tiers dans la Plateforme AutonomieCompta, il doit respecter les prescriptions légales sur l'information et/ou le consentement de ces tiers.

AutonomieCompta est autorisée par l'Utilisateur/Abonné à réutiliser, pour son propre compte, les Données Personnelles suivantes initialement traitées en tant que Sous-Traitant dans le cadre des traitements : données professionnelles du Professionnel de santé ; les données d'usage et de connexion liées à l'usage des Services d'AutonomieCompta par l'Utilisateur/Abonné ; données de gestion sans la possibilité de pouvoir identifier les patients. La finalité de cette réutilisation est d'améliorer les Services, de produire des statistiques qui pourraient être communiquées au public et à des tiers, et d'anonymiser les Données Personnelles listées.

AutonomieCompta s'engage à permettre aux personnes concernées d'exercer leur droit d'opposition. L'Utilisateur/Abonné qui ne souhaite pas autoriser cette réutilisation peut le signifier au moment de l'abonnement.

4.1. Obligations de l'Utilisateur/Abonné

L'Utilisateur et/ou l'Abonné, en sa qualité de Responsable de traitement, est seul responsable de la tenue du registre des traitements et le cas échéant de l'accomplissement des formalités préalables à la mise en œuvre du traitement de Données à

caractère personnel et Données de santé auprès de la CNIL. Il appartient également à ce dernier d'informer les Patients de l'intégration de leur Données à caractère personnel et Données de santé dans la Plateforme AutonomieCompta ainsi que des modalités d'exercice de leurs droits en mettant à disposition de ces derniers une fiche d'information.

En tant que Responsable de traitement, l'Utilisateur et/ou l'Abonné est seul responsable de l'exactitude, de la fiabilité et de la pertinence des Données à caractère personnel et Données de santé. Il est notamment responsable de l'utilisation de la Plateforme AutonomieCompta et des Documents qu'il dépose, stocke, consulte et sort de l'espace de stockage. Il lui incombe de faire toutes les déclarations nécessaires. L'Utilisateur et/ou l'Abonné s'engage à indemniser AutonomieCompta, ses représentants, ses employés et ses sous-traitants et à les décharger de toute responsabilité quant à l'ensemble des réclamations, responsabilités, dommages et frais (y compris les frais de justice, honoraires et frais) imposés à ou subis par AutonomieCompta, ses représentants, employés, et sous-traitants résultant du non-respect de cette obligation.

L'Utilisateur et/ou l'Abonné s'engage à :

- Respecter et faire respecter le secret médical;
- Mettre en place une politique d'habilitation, de gestion des droits d'accès et des rôles et privilèges, permettant de garantir la confidentialité des Données à caractère personnel et Données de santé et ce conformément à la volonté des Patients et de leurs Proches ;
- Fournir à AutonomieCompta les données nécessaires à la sous-traitance, incluant la liste des Données à caractère personnel et Données de santé à traiter, la base légale de traitement, les finalités de traitements ainsi que la durée de

conservation des Données à caractère personnel et Données de santé ;

- Documenter par écrit toute instruction concernant le/les traitement(s) de Données à caractère personnel et Données de santé effectué(s) par AutonomieCompta ;
- Veiller, au préalable et pendant toute la durée du traitement, au respect par AutonomieCompta des obligations prévues par le RGPD ;
- Superviser les traitements effectués par AutonomieCompta en qualité de Sous traitant ;
- Désigner un interlocuteur privilégié chargé de représenter le Responsable de traitement et le cas échéant un délégué à la protection des Données à caractère personnel conformément aux dispositions du RGPD ;
- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD.

4.2. Obligations d'AutonomieCompta

4.2.1. AutonomieCompta s'engage à :

- Traiter les Données à caractère personnel et Données de santé suivant les finalités et le cadre défini au sein du présent Accord, et se conformer aux normes techniques et aux bonnes pratiques applicables en matière de Données à caractère personnel et Données de santé ;
- N'agir que sur la seule instruction préalable du Responsable de traitement. En cas d'impossibilité ou de difficulté dans la réalisation de certaines instructions, AutonomieCompta en informera le Responsable de traitement dans les meilleurs délais. AutonomieCompta peut formuler une demande écrite de dérogation aux instructions.

AutonomieCompta devra recueillir l'autorisation écrite, préalable et spécifique du Responsable de traitement pour pouvoir procéder à cette dérogation ;

- Ne pas faire de copie des Données à caractère personnel et Données de santé sans autorisation ou instruction du Responsable de traitement, ne pas les communiquer à des tiers et à ne pas les utiliser à des fins autres que celles spécifiées au Contrat ;

- Ne pas exploiter ou traiter pour son propre compte et/ou pour le compte de tiers, à quelque fin que ce soit et de quelque manière que ce soit, les Données à caractère personnel et Données de santé qui lui sont confiées par le Responsable des traitements. Est notamment interdite, toute utilisation de ces Données de santé à des fins marketings, publicitaires, commerciales ou statistiques ;

- Mettre tous les moyens en sa possession au regard des stipulations contractuelles et des règles de l'art pour assurer la sécurité et la confidentialité des Données à caractère personnel et Données de santé qui lui sont confiées et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés et plus généralement, mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les Données à caractère personnel et Données de santé contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données sur un réseau, ainsi que contre toute forme de traitement illicite;

- Notifier dans les meilleurs délais le Responsable de traitement de toute survenance de faille de sécurité impactant directement ou indirectement les Données à caractère personnel, Données de santé ou traitements le concernant ;

- Procéder à des sauvegardes régulières des Données à caractère personnel et Données de santé ;

- Procéder régulièrement à des tests d'intrusion (ou Pentest) ;

- Maintenir les matériels nécessaires au bon fonctionnement des Services ;

- S'assurer de la confidentialité des Données à caractère personnel et Données de santé traitées ;

- Prendre en compte toute mise à jour, correction, suppression ou autres modifications communiquées par le Responsable de traitement concernant les Données à caractère personnel et Données de santé ;

- respecter la période de conservation des Données à caractère personnel et Données de santé applicable aux finalités pour lesquelles elles ont été collectées ou fournies et les supprimer/anonymiser dès lors que ces finalités n'existent plus, sous réserve des obligations légales ;

- Désigner un délégué à la protection des Données à caractère personnel.

4.2.2. Par ailleurs, AutonomieCompta s'engage à veiller à ce que les personnes autorisées à traiter les Données à caractère personnel et Données de santé en vertu du présent Accord :

- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

- reçoivent la formation nécessaire en matière de protection des Données à caractère personnel et des Données de santé.

AutonomieCompta met en œuvre tous les moyens nécessaires pour aider le Responsable de traitement dans la réalisation d'analyses d'impact relative à la protection des Données à caractère personnel et Données de santé ainsi que pour la réalisation de la consultation préalable de l'autorité de contrôle.

AutonomieCompta met à la disposition du Responsable de traitement toutes les informations nécessaires concernant les traitements des Données à caractère personnel et Données de santé afin de l'assister dans

l'accomplissement de ses obligations légales et réglementaires en tant que Responsable de traitement conformément aux dispositions du RGPD (annexe 3.1).

En l'absence d'instruction particulière de la part du Responsable de traitement sur la nature des Données à caractère personnel et Données de santé à traiter, les finalités, la base légale ainsi que la durée de conservation, le Responsable de traitement reconnaît et accepte que celles-ci seront traitées. En tant que Responsable de traitement, l'Utilisateur/Abonné peut demander à AutonomieCompta lors de l'exécution du Contrat à ce que ces modalités soient modifiées.

5. VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

AutonomieCompta notifie au Responsable de traitement toute violation de Données à caractère personnel et/ou Données de santé dans les meilleurs délais après en avoir pris connaissance, par message électronique ou tout autre moyen de communication mis à sa disposition par le Responsable de traitement.

Cette notification est accompagnée, sur demande du Responsable de traitement, de toute documentation utile afin de permettre à celui-ci, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente et le cas échéant aux personnes concernées.

Le référent à contacter pour le traitement des incidents ayant un impact sur les Données de santé hébergées est autonomiecompta@gmail.com.

6. TENUE DU REGISTRE DES ACTIVITÉS DE TRAITEMENT

AutonomieCompta déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de traitement conformément aux dispositions du RGPD.

7. INFORMATION ET DROITS DES PERSONNES CONCERNÉES

Il appartient au Responsable de traitement d'informer les Personnes concernées (i) des traitements mis en œuvre dans le cadre des Services et de recueillir leur(s) consentement(s) dès lors que cela s'avère nécessaire en vertu de la loi applicable; (ii) des bases légales des traitements mis en œuvre, des finalités des traitements ainsi que de la liste des sous-traitants susceptibles de traiter leurs Données à caractère personnel.

Afin d'assister le Responsable de traitement dans cette information, AutonomieCompta publie sur son site une Politique de protection des données à caractère personnel.

8. GESTION DES DROITS

Il appartient au Responsable de traitement de donner suite aux demandes de droit des Personnes concernées sur leurs Données à caractère personnel.

Dans la mesure du possible, AutonomieCompta, en sa qualité de sous-traitant et sur demande du Responsable de traitement, pourra assister le Responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des Personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage), droit d'organiser le sort de ses Données à caractère personnel notamment après la mort.

Si une Personne concernée contacte directement AutonomieCompta pour exercer l'un de ses droits relatifs à ses Données à caractère personnel traitées par AutonomieCompta en qualité de Sous-traitant, AutonomieCompta s'engage à renvoyer la Personne concernée vers le Responsable de traitement afin que ce dernier puisse donner suite à sa demande.

AutonomieCompta, à la demande de celui-ci pourra assister ce dernier dans ses suites à

donner aux demandes mais ne pourra répondre directement aux demandes desdites Personnes concernées.

9. SÉCURITÉ ET CONFIDENTIALITÉ

9.1 Pour ce qui concerne les Services, AutonomieCompta met en œuvre les mesures techniques et organisationnelles appropriées liées à la sécurité conformément aux dispositions prévues par la Loi Informatique et Libertés et le RGPD, et visant à garantir un niveau de sécurité approprié face aux risques présentés par le traitement des Données à caractère personnel de l'Utilisateur/Abonné,

Pour évaluer le niveau de sécurité approprié, AutonomieCompta tiendra compte des risques pouvant résulter d'une destruction accidentelle ou illicite, d'une corruption, d'une perte, d'une modification, d'une divulgation non autorisée ou de l'accès à des Données à caractère personnel susceptibles d'être transmises, stockées ou autrement traitées, conformément aux dispositions de l'article 32 du RGPD. Les obligations visées ci-dessus ne déchargent en aucun cas l'Utilisateur/Abonné de mettre en place l'ensemble des moyens de sécurité nécessaires à la confidentialité des Documents et des Données Abonné, Données base patient, Données Utilisateurs,

Données à caractère personnel et Données de santé présentes sur la Plateforme AutonomieCompta.

Il est convenu entre les Parties que le Contrat dont fait partie le présent Accord sur la protection des données pourra être mis à disposition de la CNIL ou toute autorité compétente en cas de contrôle.

9.2 Secret Professionnel : AutonomieCompta reconnaît et accepte que les Données à caractère personnel et Données de santé traitées par le Responsable de traitement lors de l'utilisation des Services sont strictement couvertes par le secret professionnel (article 226-13 du code pénal).

9.3 Détention des données : Sauf Accord sur la protection des données exprès contraire, le Responsable de traitement demeure seul détenteur des Données Abonné/Utilisateur publiées sur la

Plateforme d'AutonomieCompta.

AutonomieCompta ne pourra revendiquer aucun droit sur les données publiées par le Responsable de traitement.

10. PERSONNEL DE AUTONOMIECOMPTA

AutonomieCompta affecte à la réalisation des Services des équipes suffisantes et qualifiées disposant des compétences techniques et/ou fonctionnelles nécessaires à la fourniture des Services. Les personnes habilitées à traiter des Données à caractère personnel et/ou Données de santé pour le compte du Responsable de traitement sont formées à la réglementation en matière de protection des Données à caractère personnel.

11. SOUS TRAITANCE ULTÉRIEURE

L'Utilisateur/Abonné concède à AutonomieCompta une autorisation écrite générale lui permettant de faire appel aux Sous-Traitants ultérieurs énumérés ici, quand cela est raisonnablement nécessaire pour fournir les Services. Conformément à cette autorisation générale, AutonomieCompta s'engage à informer chaque Utilisateur/Abonné, par le biais d'un préavis écrit de trente (30) jours, de tout changement envisagé concernant l'ajout ou le remplacement de Sous-Traitants ultérieurs, offrant ainsi à l'Utilisateur/Abonné la possibilité de soulever toute objection qu'il pourrait avoir à l'égard de ces changements. Si l'Utilisateur/Abonné a des raisons légitimes et raisonnables de s'opposer à la nomination d'un nouveau Sous-Traitant ultérieur, l'Utilisateur doit immédiatement motiver sa réclamation à AutonomieCompta en adressant un avis écrit à autonomiecompta@gmail.com, dans les trente (30) jours ouvrables suivant l'avis émis par AutonomieCompta, à défaut de quoi

l'Utilisateur/Abonné sera réputé avoir approuvé et accepté cette nomination.

Après discussions et en l'absence d'accord entre AutonomieCompta et l'Utilisateur/Abonné, l'Utilisateur/Abonné pourra, dans les trente (30) jours suivant la notification, résilier la partie du Contrat affectée par la mise à jour en question.

Concernant chaque Sous-Traitant ultérieur, AutonomieCompta : (i) fera preuve d'une diligence raisonnable sur le plan commercial dans l'évaluation, la nomination et la surveillance des activités de traitement des Sous-Traitants ultérieurs; (ii) inclura dans le contrat entre AutonomieCompta et chaque Sous-Traitant ultérieur des clauses offrant un niveau de protection équivalent pour les Données à caractère personnel et Données de santé des Abonnés/Utilisateurs ainsi que des Patients et de leurs Proches, telles que celles prévues dans le présent Accord.

Si les Sous-Traitants ultérieurs ne remplissent pas leurs obligations en matière de protection des Données à caractère personnel, AutonomieCompta demeure responsable devant le Responsable de traitement de l'exécution par les Sous-Traitants ultérieurs de ses obligations conformément aux termes du Contrat.

12. AUDIT

12.1 Afin de mesurer la sécurité des Services, le Responsable de traitement pourra faire réaliser à ses frais des audits de sécurité, dans le respect des conditions prévues au présent article et dans la limite d'un (1) audit par an et de cinq (5) jours ouvrés maximum, le temps passé par le personnel de AutonomieCompta étant facturé au Responsable de traitement.

12.2 L'audit se limitera à la vérification des processus, de l'organisation et des outils directement et exclusivement liés à la mise en œuvre des dispositions du RGPD pour les Services concernés.

L'audit ne doit en aucun cas avoir pour but de surveiller ou d'exiger l'accès (i) à toute Donnée à caractère personnel ou Donnée de santé non spécifique, qu'elle soit confidentielle ou non, ou à toute information dont la divulgation pourrait, à la discrétion de AutonomieCompta, nuire à la sécurité des Services ou d'un autre de ses Utilisateurs ; (ii) aux données financières de AutonomieCompta ; ou (iii) aux Données à caractère personnel relatives aux employés de AutonomieCompta ou de ses Sous-Traitants.

Il est convenu que toutes les activités entreprises dans le cadre d'un audit ne doivent, ni concurremment ni par ailleurs : (i) être de nature à entraver, modifier ou affecter de quelque manière que ce soit le fonctionnement de Services, systèmes, réseaux, logiciels et/ou matériels informatiques autres que ceux alloués à l'usage exclusif de l'Utilisateur/Abonné; (ii) endommager l'infrastructure hébergeant les Services; (iii) endommager, supprimer, modifier tout type de données; (iv) permettre un accès non autorisé ou la maintenance des données précitées.

Aucun test d'intrusion ou de pénétration visant la plateforme et l'application AutonomieCompta n'est autorisé pour quelque motif que ce soit et est exclu des audits sans l'accord écrit et préalable de AutonomieCompta. Tous les documents et informations nécessaires à la réalisation de l'audit seront mis à la disposition des auditeurs par AutonomieCompta exclusivement dans les locaux de celui-ci, sans qu'il n'y ait de possibilité de retrait ou de copie, à quelque fin que ce soit. Cette interdiction s'appliquera également aux documents et informations mis à disposition par les Sous-Traitants de AutonomieCompta. Sur demande du Responsable de traitement, AutonomieCompta communiquera à celui-ci les rapports d'audit de certification délivrés par l'organisme de certification destinés à une telle communication.

12.3 Le Responsable de traitement devra faire parvenir à AutonomieCompta au minimum trente (30) jours avant la réalisation de l'audit une convention d'audit détaillant son périmètre exact, les dates et horaires prévus, les conditions y afférent. L'auditeur devra également préciser, les éventuels comptes et profils utilisés pour les tests (adresse IP sources, user agent etc), la méthodologie employée, ainsi que les acteurs qui seront audités. Le contenu de la convention d'audit doit être accepté préalablement par AutonomieCompta avant tout début d'audit.

12.4 Les informations obtenues au cours de l'audit sont des Informations Confidentielles et devront être traitées comme telles par le Responsable de traitement. Ces informations pourront uniquement être communiquées aux personnes soumises à des exigences fortes en matière de confidentialité et ayant un intérêt direct et majeur à les connaître et ne devront en aucune manière être divulguées au public ou en interne. Si le Responsable de traitement souhaite faire appel à un auditeur externe, le Responsable de traitement devra obtenir l'accord préalable écrit de AutonomieCompta, étant entendu que AutonomieCompta ne pourra refuser ledit auditeur qu'en faisant valoir des arguments objectifs et fondés.

L'auditeur externe ne pourra en aucun cas être un concurrent de AutonomieCompta et devra s'engager par écrit au respect des conditions fixées au présent article.

Le Responsable de traitement s'engage à communiquer gratuitement le rapport d'audit à AutonomieCompta qui pourra présenter ses observations.

AutonomieCompta disposera d'un délai raisonnable à compter de la réception du rapport pour corriger les manquements et/ou non-conformités constatés.

13. RÉCUPÉRATION DES DONNÉES

L'Abonné et l'Utilisateur pourront récupérer les Données à la fin du Contrat, sauf dans le cas où

ces données auraient été collectées de façon illicite par l'Abonné et/ou l'Utilisateur. Ces données seront mises à disposition de l'Utilisateur/Abonné dans un format garantissant leur interopérabilité. La demande d'export doit être faite par email à l'adresse suivante: autonomiecompta@gmail.com

AutonomieCompta s'engage à tenir à disposition de l'Utilisateur/Abonné, pendant toute la durée du Contrat et pendant toute la durée du processus de récupération des données, une copie de celles-ci. En cas de suspension de l'accès de l'Utilisateur/Abonné aux Services AutonomieCompta, quelle qu'en soit la cause, AutonomieCompta met l'Utilisateur en mesure de récupérer, par tout moyen et sur tout support, la dernière copie de ses Données (sauf dans le cas où ces données auraient été collectées de façon illicite par l'Utilisateur).

A la fin du Contrat et sur demande formelle du Responsable de traitement, AutonomieCompta s'engage également à détruire les Données à caractère personnel de santé sans en garder de copie, sous réserve d'obligations de conservation légales auxquelles AutonomieCompta serait soumise. La politique de destruction des Données à caractère personnel de santé peut être communiquée sur demande du Responsable de traitement.

15. TRANSFERTS DE DONNEES A CARACTERE PERSONNEL

Les Données à caractère personnel peuvent faire l'objet, pour les finalités listées dans le présent Accord sur la protection des données personnelles, d'un transfert à destination des sociétés du groupe de AutonomieCompta, leurs sous-traitants ou prestataires établis dans des pays bénéficiant d'un niveau de protection adéquat ou offrant des garanties adéquates concernant la protection de la vie privée et des libertés et droits fondamentaux des personnes, et ce conformément à la législation applicable.

AutonomieCompta informe l'Utilisateur/Abonné que les Données à caractère personnel peuvent aussi être transférées par AutonomieCompta vers des pays tiers à des Sous-Traitants ultérieurs, uniquement lorsqu'un tel transfert est requis pour l'exécution des Services commandés. La liste des Sous traitants ultérieurs est disponible en annexe.

Si le transfert a lieu vers un pays tiers dans lequel la législation n'a pas été reconnue comme offrant un niveau de protection adéquat des Données à caractère personnel, AutonomieCompta veille à ce que les mesures adéquates soient mises en place conformément à la Loi Informatique et Libertés et au RGPD, et notamment, lorsque nécessaire à ce que des Clauses Contractuelles Types ou des clauses ad hoc équivalentes soient intégrées dans le contrat conclu entre AutonomieCompta et le Sous-Traitant ultérieur.

En sa qualité de Sous-traitant, AutonomieCompta s'engage à héberger ou faire héberger les Données à caractère personnel sur le territoire de l'Union Européenne et, le cas échéant, à reporter, sur le prestataire hébergeant les Données à caractère personnel, l'ensemble des obligations stipulées au sein du présent Accord.

Par ailleurs, à la demande d'autorités administratives et judiciaires habilitées, AutonomieCompta est susceptible de communiquer des Données à caractère

personnel qu'elle traite au nom et pour le compte du Responsable de traitement afin de respecter ses obligations légales. Dans ce cas, et sauf disposition légale contraire, AutonomieCompta s'engage à notifier le Responsable de traitement de cette communication.

16. CONTACT

En cas de questions sur le traitement des Données à caractère personnel et Données de santé effectué par AutonomieCompta conformément aux stipulations contractuelles, l'Utilisateur/l'Abonné peut contacter le DPO de AutonomieCompta à l'adresse autonomiecompta@gmail.com

17. LOI APPLICABLE

L'Accord est régi et interprété conformément à la législation nationale applicable au Responsable du traitement.

18. INTÉGRALITÉ DE L'ACCORD

Le présent Accord constitue l'intégralité de l'accord entre les Parties en ce qui concerne son objet et remplace tous les accords antérieurs ou contemporains entre les Parties ayant le même objet, y compris toute version antérieure d'accord sur la protection des données à caractère personnel qui aurait été signée entre l'Utilisateur/Abonné et AutonomieCompta.

ANNEXE 1 : DÉTAILS SUR LE TRAITEMENT DES DONNÉES PERSONNELLES

Cette Annexe 1 contient certains détails relatifs au traitement des Données à caractère personnel et Données de santé, conformément à l'article 28(3) du RGPD.

RESPONSABLE DE TRAITEMENT : l'Abonné ayant souscrit un Abonnement AutonomieCompta et/ou l'Utilisateur ayant un Compte Utilisateur AutonomieCompta.

Les traitements mis en œuvre doivent répondre à un objectif précis et être justifiés au regard des missions et des activités des Acteurs de santé.

SOUS-TRAITANT(S) : AutonomieCompta

Les activités effectuées par le Sous-traitant pour le compte des Responsables de traitement sont décrites ci-dessous.

TRAITEMENT N°1 : PARAMÉTRAGE DES COMPTES ABONNÉS ET UTILISATEURS

OPÉRATIONS DE TRAITEMENT :

Les Services AutonomieCompta impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel listées ci-dessous.

FINALITÉS DU TRAITEMENT :

- Gestion des comptes : paramétrer le Compte Utilisateur et les habilitations des Utilisateurs;
- Support technique et assistance : Assurer le support technique, la maintenance et le traitement des demandes des Utilisateurs, le conseil, le stockage, l'hébergement et les autres services fournis aux Utilisateurs ;
- Support Données à caractère personnel : Assistance dans la gestion des violations de Données à caractère personnel et Données de santé, assistance dans la construction de PIA, accompagnement pour répondre aux demandes d'exercice de droits des Personnes concernées ;

BASE LÉGALE DU TRAITEMENT :

Il appartient au Responsable de traitement de déterminer cette base légale avant toute opération de traitement.

Afin d'aider le Responsable de traitement, la CNIL a mis à disposition un référentiel qui propose, à titre indicatif, l'intérêt légitime comme base légale. Le Responsable de traitement est libre de mentionner à AutonomieCompta une autre base légale.

PERSONNES CONCERNÉES :

Abonné et Utilisateur tels que définis dans le Contrat.

TYPES DE DONNEES A CARACTERE PERSONNEL : Dans un souci de minimisation des Données à caractère personnel traitées, le Responsable de traitement doit veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de traitement de gestion médicale et administrative de sa patientèle.

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

a) L'identité et coordonnées de l'Acteur de santé: Genre, nom, prénom, numéro de téléphone et email, adresse postale,

b) Données professionnelles : spécialité

c) Les données d'utilisation et de connexion liées à l'usage de la Plateforme AutonomieCompta par l'Utilisateur/Abonné.

Sauf instruction particulière de la part du Responsable de traitement, AutonomieCompta traite toutes les Données à caractère personnel mentionnées ci-dessus afin de fournir le Service, objet du Contrat.

DESTINATAIRES ET SOUS TRAITANTS ULTÉRIEURS:

Se référer à la liste mentionnée à l'article 11 du présent Accord.

DURÉE DE CONSERVATION:

Une durée de conservation précise des données doit être fixée par le Responsable de traitement et communiquée à AutonomieCompta. A défaut d'une telle instruction de la part du Responsable de traitement, AutonomieCompta appliquera les durées de conservations telles que recommandées par la CNIL ou la législation applicable.

ANNEXE 2 : MESURES TECHNIQUES ET ORGANISATIONNELLES

Annexe 2- A : Mesures techniques et organisationnelles standard

[Note : cette annexe 2-A est applicable par défaut (hors cas où un Connecteur entre la Plateforme et les systèmes d'informations tiers est mis en place - ce cas est régi par l'annexe 2-B. Pour plus de précisions sur l'annexe applicable, se référer au Contrat d'Abonnement.]

SÉCURITÉ DU PRODUIT

Politique de mot de passe : composés d'au minimum 8 caractères parmi les chiffres, symboles, lettres et majuscules, les mots de passe les plus classiques sont interdits (par exemple login, nom, simples suites de chiffres). Le mot de passe doit valider un test de complexité calculé dynamiquement analysant la difficulté de le casser.

L'Utilisateur doit utiliser son Identifiant de connexion et son mot de passe pour accéder aux Services.

Processus de récupération : Les comptes peuvent être récupérés de deux manières :

1. Reset de mot de passe par email
2. Reset de mot de passe par SMS avec le support AutonomieCompta sur vérifications des informations du compte avant de permettre sa récupération.

Traçabilité des actions : Les actions des différents Utilisateurs d'une organisation sont consignées et journalisées.

SÉCURITÉ DE LA PLATEFORME

- Mises à jour de sécurité automatiques : les correctifs de sécurité sont qualifiés et appliqués automatiquement sur nos composants.

- Systèmes d'exploitation à jour et renforcés.

- Veille en sécurité : nous surveillons en continu les menaces, vulnérabilités ou vecteurs d'attaques, qu'ils soient connus ou nouveaux.

- Pare-feux et systèmes de filtrage des accès dédiés (proxy, vpn...). Protection contre les attaques de déni de service distribuées (DDoS).

Protection contre les attaques logicielles (WAF).

- Traçabilité : nous enregistrons toute action, surveillons et alertons pour tout événement de sécurité.

CHIFFREMENT DES DONNÉES

L'intégralité de nos bases de données est chiffrée au repos.

Les clés de chiffrement sont chiffrées avec une clé maître créée selon les règles de l'art et sont hébergées au sein d'un dispositif matériel sécurisé.

Les Documents sont protégés par différentes techniques de chiffrement.

Ces données ne peuvent être visibles que pour l'Utilisateur.

Liste des sous-traitants

Dernière mise à jour : Mai 2024

Dans le cadre de la fourniture de ses services, AutonomieCompta fait appel à des prestataires. Ces derniers peuvent avoir accès aux données à caractère personnel collectées par AutonomieCompta uniquement dans le cadre et pour les besoins des opérations mentionnées ci-dessous.

AutonomieCompta veille à ce que chacun de ces prestataires mette en place des mesures techniques et organisationnelles appropriées pour garantir la sécurité et la confidentialité des données traitées.

En cas de transfert en dehors de l'EEE - Espace économique européen (lorsque le serveur se trouve en dehors de l'EEE) ou en cas de risque d'un tel transfert (lorsque le serveur se trouve dans l'EEE mais que le pays d'origine du prestataire de services se trouve en dehors de l'EEE), AutonomieCompta recourt aux services du prestataire sur la base d'un instrument de transfert conforme au Règlement général sur la protection des données (RGPD) et met en place des mesures supplémentaires pour garantir un niveau de protection des données équivalent à celui du RGPD.

Conformément au RGPD et dans un souci de transparence, AutonomieCompta communique ci-dessous la liste de ses sous-traitants.

Hébergement :

Sous-Traitant	Pays d'origine du prestataire	Localisation des serveurs	Catégorie de service concerné	Type de tâche effectué
Firebase	USA	USA	Hébergement	Hébergement des données de service