CONFORMITE RGPD

AATLANTIDE

Identité du document			
Titre	Conformité RGPD Aatlantide		
Type	Avenant CGV/CGU		
Référence	RGPD_AAT		
Rédacteur	Thomas GIRARDOT		
Approbateur	Jean-pierre DENIS		
Versions	1.0	02/05/2018	Version initiale
	2.0	31/10/2021	Refonte globale du document
	3.0	17/02/2022	Refonte globale du document

	Conformité RGPD Aatlantide	RGPD_AAT
		V3.0
		17/02/2022

SOMMAIRE

1 TERMINOLOGIE

Le terme « **Nous** » désigne la société Aatlantide

Le terme « **Vous** » désigne le client en contrat avec la société Aatlantide

Le terme « **Donnée personnelle** » désigne toute information relative à une personne physique identifiée ou identifiable.

Le terme « **personne identifiable** » désigne une personne pouvant être identifiée, que ce soit directement ou indirectement, en particulier par le biais d'un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou par le biais d'un ou plusieurs facteur(s) spécifique(s) à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale d'une personne physique.

Les termes « **Responsable de traitements** » et « **Sous-traitants** » sont à comprendre au sens prévu par le chapitre IV du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

Le terme « **Sous-traitant indirect** » désigne le sous-traitant d'un sous-traitant.

Le terme « **Traitement** » désigne une opération portant sur des données personnelles ou sensibles, quel que soit l'outil ou le procédé utilisé.

Le terme « **Produit Aatlantide** » désigne l'ensemble des produits et services proposés par Aatlantide.

2 GESTION DES DONNEES FOURNIES A AATLANTIDE

2.1 TYPES DE DONNEES TRAITEES

Dans le cadre du contrat qui nous lie, Vous êtes définis comme responsable de traitement et Nous comme votre sous-traitant. De fait et afin de répondre aux besoins contractuels et légaux, différents types de données sont stockés sur nos serveurs ou ceux de nos sous-traitants :

- Données issues d'opérations techniques
- Données contractuelles
- Données d'inscription
- Données de patientèle

Le stockage et le traitement des données personnelles communiquées à Aatlantide au cours de la relation professionnelle et contractuelle sont uniquement effectués en vue d'honorer le contrat, en particulier le traitement des commandes et le service à la clientèle.

Ces données ne peuvent être utilisées à des fins d'enquêtes sur les produits et de marketing que si elles sont autorisées par le biais d'une déclaration de consentement.

Les données ne seront pas transférées ou vendues à des tiers, à moins que cela ne soit clairement requis pour respecter les obligations contractuelles ou que Vous ayez donné votre accord explicite par le biais d'une déclaration de consentement.

2.2 CATEGORIES DE PERSONNES CONCERNEES

Les données issues d'opérations techniques, contractuelles et d'inscription, concernent les utilisateurs des Produits Aatlantide.

Les données de patientèle concernent vos patients.

2.3 DONNEES ISSUES D'OPERATIONS TECHNIQUES

Les données issues d'activités techniques sont requises afin de pouvoir fournir les services convenus contractuellement. Nous collecterons des données issues de ces activités techniques à cette fin uniquement. Nous vérifions périodiquement que seules les données requises pour réaliser et améliorer les activités techniques relatives à votre produit/à vos services, sont collectées, stockées et traitées.

Lors de l'utilisation de nos services en ligne, les données suivantes, nécessaires au maintien de l'intégrité et de la sécurité du système, sont stockées temporairement (date et heure d'accès, adresse IP, adresse MAC, nom du poste, configuration du poste (RAM, processeur, résolution, …), système d'exploitation, version des pré-requis Acteur).

2.4 DONNEES CONTRACTUELLES ET D'INSCRIPTION

Les données contractuelles et d'inscription permettent d'identifier et de gérer la relation contractuelle entre Vous et Nous. Ces données comprennent tout ou partie des informations suivantes :

- Les données relatives au cabinet/établissement médical (nom de la structure, adresse de la structure, type de structure, numéro FINESS, RIB/IBAN/BIC, mandat de prélèvement SEPA)
- Les données relatives aux utilisateurs (civilité, nom, prénom, adresse électronique professionnelle, n° RPPS ou ADELI, profession, fonction, numéro AM, adresse postale, numéros de téléphone)

2.5 DONNEES DE PATIENTELE

Les données de patientèle peuvent être collectées automatiquement au moyen de dispositifs permettant la lecture de cartes physiques ou dématérialisées, récupérées via des services intégrés aux Produits Aatlantide auprès des services de la CPAM, récupérées via des interfaces avec des logiciels tiers et/ou peuvent être saisies manuellement par le personnel de la structure.

Il existe trois types de données :

- Les données nécessaires à l'exécution des obligations contractuelles ou légales
- Les données supplémentaires non obligatoires, divulguées par le patient
- Les données sensibles, soumises à un niveau élevé de protection conformément au Règlement Général sur la Protection des Données (RGPD).

L'intégration des données dans le dossier médical du patient découle de l'obligation légale du médecin de documenter toute intervention et ses résultats respectifs ayant trait au traitement actuel ou futur d'un patient.

2.5.1 DONNEES OBLIGATOIRES

- Informations d'identité (civilité, prénom, nom, genre, date de naissance, rang de naissance)
- NIR
- Si différent du patient, informations de l'assuré
- Informations relatives au centre payeur (régime, caisse, centre)
- Type de couvertures obligatoire et complémentaire
- Conditions de prise en charge
- Selon le cas, identification du médecin traitant

2.5.2 DONNEES NON-OBLIGATOIRES

- Numéro de téléphone
- Adresse postale
- Adresse email
- Contacts

2.5.3 DONNEES SENSIBLES

Afin d'assurer l'intégrité des données saisies, seul le praticien ayant rédigé le document intégré au dossier médical du patient est en mesure de le rectifier ou de l'effacer et ce dans un délai de 24h. Passé ce délai, plus aucune modification ne sera possible.

Il est possible d'exporter les données (portabilité des données) sous un format courant et lisible par une machine afin de les transmettre à un patient sur demande. Les procédures et fonctionnalités correspondantes sont décrites dans les supports utilisateurs des Produits Aatlantide.

- Antécédents
- Diagnostics
- Examens
- Résultats d'examens
- Conclusions
- Traitements et leurs résultats respectifs
- Interventions et leurs résultats respectifs
- Conseils relatifs au traitement
- Déclarations de consentement
- Lettres et demandes d'orientation vers un spécialiste

2.6 STOCKAGE DES DONNEES TRAITEES

Les données contractuelles et issues d'opérations techniques, sont stockées sur nos serveurs à Meylan (38) en France.

Les données d'inscription et de patientèle sont stockées sur les serveurs de nos sous-traitants certifiés hébergeurs de données de santé (HDS).

2.7 DUREE DE CONSERVATION DES DONNEES

Les données contractuelles sont conservées dans la limite des contraintes exigées par le droit commercial et fiscal, qui s'étendent au-delà de la résiliation du contrat.

L'ensemble des données d'inscription sont conservées jusqu'à un mois après la cessation du contrat entre Vous et Nous afin de garantir la bonne restitution des données. En cas de départ d'un utilisateur avant la fin du contrat, ses accès sont fermés mais ses données sont conservées au même titre que les utilisateurs actifs et ce à des fins de suivi d'opération. Toutefois, s'il le souhaite, il est en capacité de faire valoir ses droits à l'oubli et à la rectification dans la limite des obligations légales dues à ses fonctions.

Les données d'exploitation technique, sont utilisées en vue de garantir la sécurité des systèmes d'information et sont conservées le temps nécessaire au bon fonctionnement technique des Produits Aatlantide. Elles seront supprimées au plus tard dans un délai de 6 mois après la résiliation du contrat.

2.8 RESTITUTION DES DONNEES

Conformément au droit à la portabilité prévu par le RGPD, vous recevrez sur demande ou à échéance du contrat, vos données dans un format structuré, couramment utilisé et lisible par machine (ordinateur).

2.9 SOUS-TRAITANTS INDIRECTS

Nous faisons appel à des sous-traitants indirects pour les seuls besoins de l'exécution du contrat. Nous nous assurons que ces sous-traitants indirects soient tenus aux exigences vis-à-vis de la protection des données personnelles qui leur sont confiées et disposent de mesures techniques et organisationnelles conformes au RGPD.

Nos sous-traitants sont :

- HEXANET pour l'hébergement des données de patientèle et d'inscription
  allée Albert Caquot - CS 90001
  51686 REIMS CEDEX
- SYNAAPS pour l'hébergement des données de patientèle et d'inscription
  49 avenue Albert Einstein – BP 12074
  69603 VILLEURBANNE CEDEX
- SFR pour l'envoi des rappels SMS et la gestion du support téléphonique
  16 rue Gal Boissieu
  75015 PARIS
- ZenDesk pour la gestion des tickets d'intervention
  266 Place Ernest Garnier
  34000 MONTPELLIER
- XSALTO pour l'hébergement de notre site aatlantide.com
  6 avenue Pierre de Coubertin
  38170 SEYSSINET-PARISET

3 GESTION DES DONNEES ISSUES DES PRODUITS AATLANTIDE

3.1 VOS ENGAGEMENTS EN TANT QUE RESPONSABLE DE TRAITEMENT

En qualité de responsable de traitement, Vous êtes seul responsable de l'usage qui est fait des Produits Aatlantide dans le cadre de votre activité professionnel. Qu'il s'agisse de la collecte, du stockage, du traitement et plus généralement de toutes utilisations d'informations, à caractère personnel ou non. De fait, Vous vous engagez à :

- Obtenir le consentement exprès de vos patients avant la collecte de leurs données personnelles et à être en mesure de fournir la preuve de ce consentement
- Prendre toutes les mesures nécessaires pour fournir à vos patients toutes informations requises par la Loi n°78-178 du 6 janvier 1978 dite « Informatique et Libertés » et le RGPD, notamment à les informer de cette collecte et des finalités du traitement, ainsi qu'à les informer des droits qui leurs sont ouverts par les lois et règlements applicables en matière de protection des données à caractère personnel
- Veiller à l'accomplissement de toutes formalités, de l'obtention de toutes autorisations et de la mise en œuvre de toutes obligations légales ou réglementaires en découlant, y compris déclaratives, de tenue de registres, de notifications ou d'informations, d'analyses d'impact, de consultation préalable des autorités de protection des données à caractère personnel
- Veiller à ce que votre personnel, ainsi que vos autres sous-traitants, pouvant intervenir sur les données personnelles en lien avec le contrat, respectent ces dispositions
- Prendre toutes mesures techniques et organisationnelles nécessaires à la sécurité du traitement

3.2 NOS ENGAGEMENTS EN TANT QUE SOUS-TRAITANT

En tant que sous-traitant, Nous sommes amenés à accéder, transporter ou stocker des données à caractère personnel que Vous nous fournissez et ce dans le cadre de l'exécution des prestations de service du contrat qui nous lie. De fait, Nous nous engageons à :

- Ne traiter les données personnelles que sur instruction documentée de votre part
- Veiller à ce que les personnels autorisés à traiter les données personnelles s'engagent à respecter la confidentialité et ne les traitent que sur instruction de votre part
- N'effectuer aucun transfert des données personnelles vers un pays en dehors de l'Union Européenne, ou à défaut, à vous en informer ainsi qu'à prendre toutes mesures prescrites par les lois et règlements en vigueur afin de garantir la protection de ce transfert
- Mettre à votre disposition toutes les informations nécessaires pour démontrer le respect des obligations prévues à la présente charte, notamment pour permettre la réalisation d'audits, vous porter assistance et sous réserve de faisabilité, vous permettre de garantir l'exercice des droits des personnes concernés par le traitement
- Supprimer ou vous retourner, selon votre choix, toutes données personnelles qui seraient en notre possession au terme du contrat
- Vous notifier toute violation de données personnelles dans les meilleurs délais

4 MESURES TECHNIQUES ET ORGANISATIONNELLES

4.1 ENGAGEMENT DE CONFIDENTIALITE ET FORMATIONS

Nous nous assurons, par le biais d'une clause de confidentialité incluse au contrat de travail de nos employés, que chaque personnel ayant accès à des données personnelles ou sensibles, des données contractuelles, des données du journal et des données provenant d'opérations techniques, respecte les contraintes imposées par le RGPD.

De plus, Nous mettons en œuvre régulièrement, des formations internes afin que chaque employé ait connaissance des bonnes pratiques liées au respect de la protection des données.

4.2 GESTION DES DROITS DES PERSONNELS AATLANTIDE

Un mécanisme de gestion des droits est mis en place afin de ne permettre l'accès aux différents types de données qu'aux personnes amenées à travailler sur celles-ci et ce uniquement à des fins contractuelles.

Chacune de ces personnes est identifiée et leurs accès sont immédiatement clôturés en cas de départ d'Aatlantide.

4.3 GESTION DES DROITS DES UTILISATEURS

Les accès aux Produits Aatlantide sont créés par des personnels d'Aatlantide habilités.

L'accès au dossier médical des patients est garanti par des moyens d'authentification conformes aux référentiels de sécurité prévus par l'article L.1110-4-1 du code de la santé publique, à savoir par lecture d'une CPS ou par envoi d'un code de confirmation unique sur un média du professionnel de santé.

4.4 CHIFFREMENT DES DONNEES PATIENTS

Toutes les données à caractère personnel des patients sont chiffrées sur les serveurs de nos sous-traitants et le déchiffrement n'est opéré que sur le poste de l'utilisateur final.

4.5 SECURISATION DES DONNEES

Afin d'assurer la sécurité des données, Nous examinons régulièrement l'état de nos technologies en matière de sécurité. Les actions effectuées dans ce cadre comprennent l'analyse des scénarios catastrophes typiques, la réévaluation des besoins de sécurité/niveaux de sécurité pour les différents types de données personnelles, la répartition en différentes catégories de dommages potentiels, ainsi que la conduite d'une évaluation des risques.

Nous soumettons régulièrement nos systèmes à des tests d'intrusion afin d'évaluer l'efficacité des mesures techniques et organisationnelles en place et d'assurer la sécurité de nos processus.

4.6 SAUVEGARDE DES DONNEES ET RESILIENCE

Les données issues d'opérations techniques et contractuelles sont sauvegardées régulièrement et redondées sur un site distant afin d'éviter les pertes de données.

Les données de patientèle et d'inscription étant quant à elles hébergées chez nos sous-traitants certifiés HDS, la sécurité de ces données est conforme aux exigences qui y sont liées.

4.7 PRIVACY BY DESIGN / PRIVACY BY DEFAULT

Conformément à l'article 25 du RGPD, Nous intégrons les concepts de Privacy by design et de Privacy by default afin que les principes de protection des données, de confidentialité et de sécurité des données soient pris en compte tout au long des processus de conception et de développement des systèmes informatiques.

Les produits Aatlantide sont livrés avec des paramètres par défaut optimisés pour la confidentialité des données, de sorte que seules les données personnelles nécessaires à la finalité du traitement soient traitées.

4.8 ADMINISTRTAION A DISTANCE

A des fins de maintenance ou de support client, et uniquement dans le cadre du contrat, les employés d'Aatlantide peuvent être amenés à accéder à distance aux données des cabinets médicaux, utilisateurs et/ou patients. Cet accès est régi par les règles générales d'Aatlantide :

- L'accès à distance est fermé par défaut. Son accès à distance exige le consentement explicite de l'utilisateur et lui permet de visualiser en temps réel les interventions
- Les interventions critiques sont sécurisées par une procédure en présence de deux personnes (la procédure « des quatre yeux ») avec un personnel qualifié supplémentaire
- Les opérations d'accès à distance sont notées au sein du système informatique de relation clients d'Aatlantide. Les informations suivantes sont conservées : personne en charge de l'opération, dates et horaires, système impliqué, outil d'accès à distance utilisé, brève description des tâches effectuées et, en cas d'intervention critique, le nom des personnels qualifiés additionnels consultés lors de la procédure
- L'enregistrement d'identifiants quel qu'ils soient est strictement interdit

4.9 VIOLATION DE DONNEES

Nous nous engageons à notifier immédiatement au responsable de traitement toute violation de données à caractère personnel dès lors qu'elle a été détectée par nos services.

Cette notification est accompagnée de toute documentation utile afin de Vous permettre, de notifier cette violation à l'autorité de contrôle compétente.

En particulier, Nous veillerons à communiquer :

- La description de la nature de la violation de données à caractère personnel
- Les catégories de données
- Le nombre approximatif de personnes concernées par la violation
- Les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés
- Décrire les conséquences probables de la violation de données
- Préciser les mesures prises ou à prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives
- Le nom et les coordonnées du délégué à la protection des données auprès duquel des informations supplémentaires peuvent être obtenues

5 DROITS DE LA PERSONNE CONCERNEE

5.1 DELEGUE A LA PROTECTION DES DONNEES (DPO)

Le Délégué à la Protection des Données peut être contacté pour toute question relative au traitement des données personnelles et pour la réception des demandes d'informations ou plaintes.

CompuGroup Medical
Jean-Pierre DENIS
Délégué à la Protection des Données
55, av. des Champs Pierreux
92012 Nanterre cedex
dpo.fr@cgm.com

5.2 TRAITEMENT DES DONNEES UTILISATEURS PAR AATLANTIDE

Chaque utilisateur a le droit d'être informé des données stockées le concernant, d'en demander la rectification, l'effacement, la restriction du traitement, la portabilité et de s'opposer à leur traitement. À tout moment, l'utilisateur peut revenir sur son consentement au traitement de ses données.

Toutefois la rectification, la limitation du traitement ou l'effacement de ces données peut empêcher l'utilisation de certaines fonctionnalités ou être limité par des exigences légales tel que le suivi des opérations réalisées sur un dossier médical.

S'il souhaite faire valoir ses droits, il doit contacter le DPO comme indiqué au paragraphe 5.1.

Si l'utilisateur estime que Nous ne traitons pas ses données personnelles de manière appropriée ou si une demande de rectification, limitation ou d'effacement de données n'a pas été traitée dans le délai d'un mois comme prévu par le RGPD, l'utilisateur a le droit de déposer une plainte auprès des autorités de surveillance responsables.

5.3 TRAITEMENT DES DONNEES DE PATIENTELE

Un patient a le droit d'être informé des données stockées le concernant, d'en demander la rectification, l'effacement, la restriction du traitement, la portabilité et de s'opposer à leur traitement. À tout moment, le patient peut revenir sur son consentement au traitement de ces données. Le retrait prend effet pour l'avenir.

Lorsque le responsable de traitement reçoit une demande d'effacement de la part d'un patient, il est néanmoins tenu de respecter les périodes de conservation applicables.

Si le patient estime que le responsable de traitement ne traite pas ses données personnelles de manière appropriée ou si une demande rectification, limitation ou d'effacement de données n'a pas été traitée dans le délai d'un mois comme prévu par le RGPD, l'utilisateur a le droit de déposer une plainte auprès des autorités de surveillance responsables.

5.4 AUTORITE DE CONTROLE COMPETENTE

L'autorité de contrôle compétente pour Aatlantide est la Commission nationale de l'informatique et des libertés de France.

https://www.cnil.fr