DEMARCHE DE MISE EN CONFORMITE RGPD

MAI 2018

TABLE DES MATIERES

1 OBLIGATIONS GENERALES

La société Aatlantide est sous-traitante de données de santé à caractère personnel, et la nature des opérations réalisées sur les données sont le stockage, la consultation et la modification de données dans le cadre de :

- La tierce maintenance applicative du logiciel, comprenant la maintenance corrective, la maintenance évolutive, la mise en conformité par rapport à la règlementation, l'adaptation aux nouvelles technologies, la maintenance du SGBDR.
- La fourniture et la mise en œuvre de modules ou licences complémentaires.
- Les prestations complémentaires dans la mesure où elles nécessitent l'accès aux données personnelles.

La société Aatlantide héberge l'ensemble de ses données sur le territoire français, conformément à son agrément ministériel d'Hébergeur de données de santé à caractère personnel, et à la note d'information n°2016/004 du 5 avril 2016 relative à l'informatique en nuage du SIAF.

La société Aatlantide est agréée pour une prestation d'hébergement de données de santé à caractère personnel gérées via ses services Acteur.fr et ActeurCS.fr depuis mars 2010. Cet agrément, délivré par le ministère de la santé, garantit la confidentialité des données à caractère personnel traitées.

Des compléments d'informations peuvent être trouvés dans nos conditions générales de vente et d'utilisation.

2 OBLIGATIONS RELATIVES AUX PERSONNELS

La société Aatlantide veille à ce que ses personnels autorisés à traiter les données à caractère personnel s'engagent à respecter la confidentialité par la signature d'une clause de confidentialité incluse dans leur contrat de travail.

Extrait du contrat de travail

Article 7 – Confidentialité

Le salarié s'engage à ne divulguer aucune information concernant les activités de la société, dont il pourrait avoir connaissance dans l'accomplissement de ses fonctions et qui serait de nature à porter préjudice à l'entreprise.
Cette obligation de confidentialité s'applique tant à l'égard des tiers que des salariés de l'entreprise.
Elle gardera tous ses effets pendant toute la durée du contrat de travail et se prolongera après la rupture de celui-ci pour quelque motif que ce soit.

De plus, du fait de la nature personnelle, nominative et médicale des données liées aux prestations et services effectués par la société Aatlantide, les données auxquelles le salarié peut avoir accès sont strictement couvertes par le secret professionnel (article 226-13 du code pénal). Le salarié s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Le salarié s'engage donc à respecter les obligations suivantes :

- Ne prendre aucune copie des documents et supports d'informations qui lui sont confiés sans autorisation exprès de son supérieur hiérarchique.
- Ne pas utiliser les documents et informations traités à des fins autres que celles liées à son contrat de travail.
- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales.
- Prendre toutes mesures de sécurité, notamment matérielle, pour assurer l'intégrité des documents et informations traités.

De plus, les personnels de la société Aatlantide autorisés à traiter les données à caractère personnel reçoivent tous une formation en matière de protection des données à caractère personnel de la part du RSSI de la société. Cette formation a lieu directement après leur prise de fonction.

3 OBLIGATIONS RELATIVES A LA PROTECTION DES DONNEES DES LA CONCEPTION ET PAR DEFAUT

La société Aatlantide prend en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception de ses produits en mettant en œuvre :

- Un mécanisme de gestion des habilitations via Active Directory garantissant que seules les personnes habilitées accèdent aux seules données nécessaires à la réalisation de leurs missions. Les droits des personnes sont réexaminés périodiquement par l'équipe sécurité afin d'assurer leur pertinence.

- Des mécanismes de traitement garantissant l'archivage de données à l'issue de leur durée de conservation, ou l'anonymisation rendant impossible toute identification ultérieure. Toute demande d'archivage ou d'anonymisation doit pour l'instant faire l'objet d'une demande à l'adresse suivante : dpo@aatlantide.com. Des outils d'anonymisation et d'archivage automatiques et mis à la disposition des clients sont en cours de développement.

- Des mécanismes assurant la traçabilité des accès, afin de de permettre la détection d'éventuelles tentatives d'accès frauduleux ou illégitimes. Ces mécanismes concernent à la fois les accès au logiciel Acteur.fr (consultation possible de l'historique des actions réalisées directement dans le logiciel) et les accès réalisés par les personnels de la société Aatlantide (stockage des logs sur un serveur Syslog dédié) sur les différents matériels servant au bon fonctionnement de l'application Acteur.fr (serveurs, pares-feux, switch…).

- Des mécanismes assurant la traçabilité des accès aux données sensibles comportant l'identification de l'utilisateur et l'horodatage des opérations réalisées (consultation, modification ou suppression). Les données de journalisation sont conservées durant 2 ans puis détruites. Les mécanismes mis en œuvre sont les mêmes que ceux listés dans le point précédent.

La société Aatlantide garantie la minimisation des données traitées dans le cadre de ses activités commerciales. En ce qui concerne les données de santé, c'est le responsable du traitement qui est garant de la minimisation des données traitées.

4 OBLIGATIONS RELATIVES A LA SOUS-TRAITANCE

La société Aatlantide s'assure que ses sous-traitants présentent les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données.

Les sous-traitant de la société Aatlantide sont :

- La société Hexanet concernant l'hébergement physique de ses serveurs.
- La société SFR concernant les rappels SMS et la gestion du support téléphonique.
- La société Xsalto concernant l'hébergement de son site commercial.

5 OBLIGATIONS RELATIVES A L'EXERCICE DES DROITS DES PERSONNES

La société Aatlantide s'engage à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Toute demande de ce type peut être réalisée en envoyant un mail à l'adresse suivante : dpo@aatlantide.com. Toute demande de la part d'un patient doit passer par le responsable du traitement.

6 OBLIGATIONS RELATIVES A LA NOTIFICATION DE VIOLATIONS DE DONNEES A CARACTERE PERSONNEL

La société Aatlantide s'engage à notifier immédiatement toute violation de données à caractère personnel. Cette notification est accompagnée de toute documentation utile afin de permettre, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

En particulier, la société Aatlantide veillera 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.
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact (dpo@aatlantide.com) auprès duquel des informations supplémentaires peuvent être obtenues, de décrire les conséquences probables de la violation de données et enfin de 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.

7 OBLIGATIONS RELATIVES A LA SECURITE

La société Aatlantide s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité adapté au risque.

Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services de traitement sont :

- Un accès du professionnel de santé aux dossiers médicaux garanti par des moyens d'authentification forte conformes aux référentiels de sécurité mentionné à l'article L.1110-4-1 du code de la santé publique, à savoir après lecture de la carte de professionnel de santé (CPS) et en cas d'absence de la CPS : par envoi d'un code de confirmation unique sur un média du professionnel de santé (mail, SMS).

- Le chiffrement de toutes les données à caractère personnel sur les serveurs de la société Aatlantide et dont le déchiffrement n'est opéré que sur le poste de l'utilisateur final.

- Un système de signature garantissant l'intégrité de tous les documents stockés dans les bases de données.

- La redondance des matériels (serveurs, pares-feux, switch, alimentations…) permettant de garantir la disponibilité des données en cas de problème technique.

- Une duplication des données stockées par la société Aatlantide sur un site géographique distant qui prend le relai en cas de défaillance du site principal.

Les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique et technique sont :

- Le plan de reprise d'activité de la société (PRA) Aatlantide qui prévoit la duplication des données sur un site géographique distant pour pallier aux incidents techniques et matériels.

- La sauvegarde quotidienne des données sur un serveur isolé permettant à la société Aatlantide de se prémunir contre les corruptions volontaires de données suite à une intrusion.

L'équipe sécurité de la société Aatlantide évalue régulièrement l'efficacité des mesures techniques et organisationnelles assurant la sécurité du traitement.

8 OBLIGATIONS RELATIVES A LA SUPPRESSION DES DONNEES

Au terme de la prestation de services relatifs au traitement de ces données, la société Aatlantide s'engage à renvoyer toutes les données à caractère personnel au client. Les données sont renvoyées sous la forme d'une archive sécurisée contenant les données médicales au format XLS, les formulaires au format XPS et les documents stockés en GED dans leurs formats d'origine.

Le renvoi s'accompagne de la destruction par anonymisation de toutes les copies existantes dans les systèmes d'information de la société Aatlantide. Une fois détruites, la société Aatlantide justifie par courrier de la destruction.

9 OBLIGATIONS RELATIVES A LA TENUE DU REGISTRE ET DE LA DOCUMENTATION

La société Aatlantide tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte de ses clients :

- Le nom et les coordonnées du client pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données.
- Les catégories de traitements effectués pour le compte du client.

La société Aatlantide met à la disposition de ses clients la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le client ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Le coût de contribution d'un auditeur interne sera intégralement pris en charge par le client.

Pour toute demande d'information complémentaire, les clients peuvent envoyer un mail à l'adresse suivante : dpo@aatlantide.com.