Politique de confidentialité et de protection des données à caractère personnel

L'Hospitalisation Privée d'Addictologie (HPA) est un Réseau qui gère et développe des établissements sanitaires spécialisés dans la prise en charge des affections liées aux conduites addictives.

Dans le cadre de ses engagements en matière de la sécurité Humaine, et de la santé, du respect de l'environnement et de l'éthique dans les relations d'affaires, HPA met tout en œuvre pour garantir la vie privée, en traitant les données à caractère personnel, en conformité avec le Règlement Général sur la Protection des Données (RGPD), et sur la loi « Informatique et Libertés » du 06 Janvier 1978 dans sa version modifiée par la loi du 20 Juin 2018.
La présente politique est destinée à informer sur la manière dont la société collecte, utilise, stocke, archive et transmets les données personnelles.
Elle porte exclusivement sur les traitements crées et ou exploités par HPA directement, conjointement ou par un sous-traitant spécifiquement désigné à cet effet.

A qui s'adresse cette politique

Elle est destinée à toutes les personnes physiques en relation avec HPA, de manière directe ou indirecte et en particulier aux :

- Patients
- Visiteurs / utilisateurs du site internet
- Fournisseurs
- Prestataires de service
- Sous-traitants
- Cocontractants
- Personnel des administrations et des organismes sociaux
- Tiers institutionnels

Quelles sont les données susceptibles de faire l'objet d'un traitement ?

Au nom du principe de minimisation des données, HPA, collecte uniquement les données nécessaires suivant les besoins :

Correspondant, personne physique du cocontractant ou du prospect

- Nom et prénom
- Numéro de téléphone professionnel
- Adresse mail professionnelle

Personnels des administrations et des organismes sociaux

- Nom et prénom du gestionnaire ou de l'interlocuteur habituel
- Numéro de téléphone professionnel
- Adresse mail professionnelle

Internautes

- Adresse IP du terminal ou de l'équipement connecté à internet
- Données propres aux dispositifs techniques utilisés pour accéder aux services mis à disposition par HPA (PC, smartphones, Navigateurs Web, etc.)
- Historique de navigation
- Cookies

Visiteurs

- Nom, prénom, employeur, fonction, contact au sein de HPA

Quels sont les principes qui régissent le traitement des données personnelles ?

Le traitement des données à caractère personnelles par HPA répond aux principes suivants :

- Les données personnelles sont traitées de manière licite, loyale, transparente **(Licéité, Loyauté, Transparence).**
- Les données personnelles sont collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités **(Limitation des Finalités)**
- Les données personnelles sont conservées de manière adéquate, pertinente, et sont limitées à ce qui est nécessaire au regarde des finalités pour lesquelles elles ont été traitées **(Minimisation des données)**
- Les données personnelles sont exactes, tenues à jour et toutes les mesures raisonnables sont prises pour que les données inexactes, eu égard aux finalités pour lesquelles elles ont été traitées, soient effacées ou rectifiées sans tarder **(Exactitude)**
- HPA met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque inhérent à ses opérations de traitement, répondre aux exigences réglementaires et protéger les droits et les données des personnes concernées dès la conception des opérations de traitement **(Protection dès la conception).**

HPA impose contractuellement le même niveau de protection des données personnelles à ses sous-traitants (prestataires, fournisseurs, etc.)

Pourquoi et sur quelle base juridique HPA traite les données à caractère personnel ?

Finalité	Base juridique
- Prise de contact dans le cadre d'une démarche commerciale - Prise de contact dans le cadre d'une sollicitation commerciale - Relations d'affaires avec les clients et els fournisseurs - Relations d'affaires avec les sous-traitants et les prospects Informations sur les contacts professionnels - Conclusion, exécution, renouvellement ou dénonciation des contrats Fourniture de service en ligne	Consentement Intérêt légitime d'assurer le développement de HPA Obligations légales et contractuelles
	Obligations légales

- Gestion des relations avec les administrations fiscales et sociales	
- Analyse et sécurisation des accès au système d'information	Obligations légales et contractuelles Intérêts légitimes de HPA
- Mise en œuvre d'un dispositif de vidéosurveillance afin d'assurer la sécurité et le contrôle des accès - Contrôles des visiteurs	Obligations légales et contractuelles Intérêt légitime à sécuriser l'accès aux locaux

L'intérêt légitime de HPA peut notamment recouvrir :

- L'amélioration du fonctionnement du site Web afin qu'il réponde mieux aux attentes et besoins des utilisateurs
- La mise en place et le maintien de relations pérennes avec les prospects, clients, sous-traitants, fournisseurs, investisseurs, représentants des médias et toute autre personne intéressée par les activités de HPA.
- La sécurisation des outils (site, messagerie, objets connectés, etc.) afin d'assurer leur protection et leur sécurité et de veiller à ce qu'ils fonctionnent correctement et soient améliorés en permanence.
- La nécessité de disposer des informations nécessaires aux personnes présentes dans les locaux à l'instant T, en cas d'alerte.

Combien de temps sont conservées les données ?

HPA conserve les données personnelles pendant une durée n'excédant pas celle nécessaires aux finalités pour lesquelles elles ont été traitées.

Les durées de conservation tiennent également compte :

- Des dispositions légales applicables imposant une durée de conservation précise pour certaines catégories de données.
- Des délais de prescription ou de forclusion applicables
- De la jurisprudence
- Des recommandations de la CNIL concernant certaines catégories de traitements de données.

Données personnelles	Durée de conservation
Coordonnées des prospects	4 ans après le dernier contact sauf accord express de la personne
Correspondant personne physique du cocontractant	Temps de la relation contractuelle
Personnels des administrations et des organismes sociaux	Pendant toute la durée de la relation

Internautes	2 ans
Visiteurs	6 mois maximum

Qui a accès aux données ?

L'accès aux données à caractère personnel est autorisé pour les collaborateurs de HPA, habilités à traiter ces données selon les principes de mises à jour régulières, dans le seul but de remplir des tâches définies.

Ces collaborateurs sont soumis à une obligation de confidentialité.

Les destinataires externes sont soumis aux mêmes principes d'habilitation et à la même obligation de confidentialité.

HPA fait notamment appel à des prestataires qui fournissent des services informatiques tels que des fournisseurs de plateforme, des services d'hébergement, des services e maintenance et de support techniques pour nos bases de données ainsi que pour ses logiciels et applications qui peuvent contenir des données personnelles auxquelles ces services peuvent parfois avoir accès afin d'accomplir les tâches demandées.

HPA peut notamment communiquer des données à caractère personnel à des tiers :

- En cas de cession d'une activité ou d'actifs, à l'acquéreur potentiel de cette activité ou de ces actifs. Si HPA ou toute partie de ses actifs fait partie d'une acquisition par un tiers, les données à caractère personnel détenues concernant ses clients et liées à ces actifs sont l'un des actifs transférés.
  Le cas échéant, l'acquéreur qui agira comme le nouveau responsable du traitement traite les données et sa politique de protection régit le traitement des données à caractère personnel.

- Si HPA, est contrainte de divulguer ou partager les données à caractère personnel pour se conformer à une obligation légale, ou pour faire respecter ou appliquer ses conditions d'utilisation ou de vente ou toutes autres conditions acceptées ; ou pour protéger les droits, la propriété ou la sécurité de HPA, de ses clients, de ses fournisseurs ou de ses collaborateurs.

- Avec le consentement préalable de la personne concernée

- En application de la loi

En toute état de cause, HPA s'interdit de vendre les données à caractère personnel.

Où sont conservées les données personnelles

Toutes les données sont hébergées sur des serveurs dédiés avec toutes les mesures techniques et organisations jugées appropriées, conformément à l'article 32 du RGPD, ce, afin de garantir la sécurité et la confidentialité des données.

Les données sont hébergées dans l'Espace Economique Européen et ne sont pas transférées hors de l'UE.

Violation des données

En cas de violations de données à caractère personnel, HPA, s'engage à en informer la CNIL, dans les conditions prescrites par la RGPD.
Dans l'hypothèse où la violation fait porter un risque élevé pour les personnes concernées, HPA leur communiquera les informations et recommandations nécessaires.

Quels sont vos droits ? Et comment les exercer ?

Les lois applicables relatives à la protection des données vous donnent plusieurs droits :

- Le droit d'accès et le droit de rectification : vous disposez du droit d'accéder à vos données personnelles. Vous pouvez nous solliciter afin que vos données personnelles soient mises à jour ou rectifiées si vous démontrez que les données que nous détenons à votre sujet sont incorrectes.
- Le droit d'oubli et le droit à l'effacement : Dans certaines circonstances vous êtes autorisés à demander un traitement restreint et/ou la suppression de vos données personnelles. Cependant, ce droit est soumis aux obligations légales liées à la durée de conservation des informations ainsi qu'aux motifs légitimes liés à notre activité. Si après vérification votre demande est recevable, le réseau privé d'addictologie procédera à la suppression de vos données personnelles dans les meilleurs délais.
- Le droit d'opposition : Vous avez le droit, à tout moment, de vous opposer au traitement de vos données personnelles pour des motifs énoncés dans la loi, sans justification nécessaire. (ex : demande d'opposition à l'enregistrement vidéo)
- Le droit à la limitation : vous avez le droit d'obtenir la limitation du traitement de vos données lorsque vous vous y êtes expressément opposé, si vous démontrez que le traitement de vos données est illicite, si vous contestez la véracité de ces données, ou lorsque vous avez besoin de ces données pour constater, réaliser ou défendre vos droits en justice.

Le traitement de vos données personnelles se base sur votre consentement, vous avez de ce fait également le droit de le retirer à tout moment. Ce retrait de consentement prend effet pour le futur.

L'exercice des droits peut s'exercer à l'adresse suivante :
HPA, 31 Boulevard de la Tour Maubourg 75007 Paris, Mention : Protection des Données Personnelles
Ou par courriel à l'adresse : dpo@hp2a-group.fr

Nous procéderons alors à une vérification de votre identité.
La personne concernée doit accompagner sa demande, d'éléments nécessaires à son identification : nom, prénom, e-mail, ainsi que toute autre information nécessaire à la confirmation de son identité.
Vous avez également la possibilité de faire une réclamation relative au traitement de vos données personnelles auprès de la Commission Nationale Informatique et Libertés (CNIL) 3, place de Fontenoy, 75007 Paris.

Modification de notre clause de confidentialité

Nous nous réservons le droit de modifier à tout moment cette politique de confidentialité. Il conviendra de s'y référer autant que nécessaire et de vérifier régulièrement si des modifications ont pu y être apportées

Annexe 1 : MTO (Mesures techniques et organisationnelles)

Annexe MTO à la Convention relative au traitement des Données personnelles (selon l'Article 28 Paragraphe 3, point c, et l'Article 32 RGPD UE)

1. Contrôle d'accès aux locaux et aux installations où les données sont traitées

L'accès physique non autorisé aux locaux est strictement interdit.
Les Mesures de sécurité suivantes, conformes à l'état de l'art permettant de contrôler l'accès aux locaux et aux installations ont été mises en place :

- Verrouillage des portes
- Personnel de sécurité, vigiles, hôtesses.
- Installations de surveillance (système d'alarme, vidéo/CCTV)
- Revue régulière des autorisations permanentes d'accès. Tenue d'un registre d'intervention.

2. Contrôle d'accès aux systèmes

L'accès non autorisé aux systèmes informatiques est strictement contrôlé.
Les mesures techniques (sécurité des identifiants/mots de passe) et d'identification et d'authentification de l'utilisateur ont été mises en place :

- Procédures de mot de passe (y compris les caractères spéciaux, la longueur minimale, le changement régulier de mot de passe)
- Blocage automatique (mot de passe bloqué après plusieurs tentatives infructueuses)
- Cryptage des supports de données
- Tests de pénétration extérieure afin de vérifier de façon régulière la sécurité des traitements et des données
- Gestion de la réponse aux incidents

3. Contrôle d'accès aux données

Les activités des systèmes informatiques non couvertes par les droits d'accès attribués ne sont pas autorisées.
Les mesures suivantes qui ont été mises en place répondent aux exigences du mécanisme d'autorisation et des droits d'accès d'une part, du contrôle et de l'enregistrement des accès d'autres part :

- Droits d'accès différenciés (profils, rôles, transactions et objets)
- Rapports de connexion et droits d'accès
- Procédure de création, de modification et de suppression des utilisateurs
- Unicité du couple compte/identifiant d'utilisateur

4. Contrôle de divulgation

Les aspects de la divulgation des données à caractère personnel sont contrôlés afin d'empêcher la perte, l'altération ou la divulgation non autorisée.
Les mesures de transport, transmission et communication ou stockage des données sur les supports de données (manuels ou électroniques) ont été mises en place :

- Cryptage/canalisation (VPN=Virtual Private Network)
- Connexions sécurisées (https)
- Sécurité du transport (sftp)

5. Contrôle de la saisie

La documentation complète de la gestion et de la maintenance des données est conservée.
Les mesures de vérification ultérieure de la saisie, de la modification ou de l'enlèvement (suppression) des données, et de la personne y ayant procédé ont été mises en place :

- Systèmes de connexion et de reporting

6. Contrôle des activités

Le traitement des données sous-traitées est effectué conformément aux instructions. Aucun traitement de données par des tiers selon l'Article 28 RGPD n'est réalisé sans les instructions correspondantes du responsable de traitement.
Les mesures (techniques/organisationnelles) en vue de séparer les responsabilités entre le Responsable de traitement et le Sous-traitant ont été mises en place :

- Rédaction claire du contrat relatif au traitement (matrice de responsabilité RACI)
- Contrat écrit
- Critères de sélection du sous-traitant
- Contrôle de l'exécution du contrat
- Vérifications (audit) de suivi de surveillance

7. Contrôle de disponibilité

Les données sont protégées contre la destruction ou la perte accidentelle.
Les mesures suivantes (physiques/logiques) visant à assurer la sécurité des données ont été mises en place :

- Procédures de sauvegarde/résilience des systèmes informatiques
- Vérification continue de l'intégrité du système informatique
- Miroitage des disques durs par la technologie RAID
- Maintien permanent de l'alimentation électrique (UPS)
- Stockage des sauvegardes à distance (Remote backup)
- Systèmes de pare-feu/antivirus
- Plan de reprise d'urgence (Mise en place d'un Plan de reprise d'activité, PRA).

8. Contrôle d'isolation (dans le cadre du développement des applicatifs du Réseau)

Le traitement isolé des Données collectées à différentes fins a été mis en place :

- Support client multiple
- Bacs à sable
- Anonymisation des environnements dupliqués

9. Contrôle de séparation

Les données collectées à des fins différentes sont traitées séparément.
Les mesures permettant le traitement séparé (stockage, modification, suppression, transmission) de données à différentes fins ont été mises en place :

- Gestion de la mise en place du « client interne »
- Limitation des droits d'utilisation
- Séparation des fonctions (production/test)

10. <u>Documents et/ou certificats correspondants</u>

Les documents et/ou certificats correspondants qui peuvent prouver ou expliquer les mesures mises en œuvre sont mis à disposition des partenaires, à l'exception des documents pouvant compromettre le système de sécurité du réseau privé d'addictologie.

Fait à Paris le 1er Janvier 2021