# Politique de sécurité de l'Association pour la Psychothérapie Psychanalytique.

Remarque : par travailleurs, il faut entendre : membres, salariés, indépendants, stagiaires et bénévoles / document à communiquer aux travailleurs et aux sous-traitants

## Gestion des accès informatiques

Les personnes autorisées à avoir accès au système de traitement des données sont uniquement les personnes sous contrat de travail, les personnes ayant signé une convention d'indépendant, une convention de stage ou une convention de bénévolat avec l'ARPP. Lors de leur engagement ou lors de la signature de la convention, les travailleurs signent un *engagement de confidentialité des personnes ayant vocation à traiter des données personnelles*.

Aucun travailleur n'a le droit de donner accès au système informatique à un tiers sans le consentement du pouvoir organisateur. L'accès au système informatique est contrôlé via un login et mot de passe. Ce mot de passe ne pourra pas être noté à côté du système informatique ou communiqué à des tiers, et aucune forme de pré-enregistrement ne pourra être utilisée.

Une personne de référence concernant la sécurité informatique est désignée. Cette personne se charge de créer des comptes utilisateurs spécifiques pour chaque travailleur et communique les codes d'accès à la direction afin de pouvoir modifier les accès lors d'un changement de personnel ou d'une absence prolongée.

Les ordinateurs sont programmés pour se mettre en veille à partir de 5 minutes d'inutilisation et il faut réintroduire le mot de passe pour rouvrir la session.

En fin de journée, les comptes utilisateurs doivent d'être déconnectés et les ordinateurs éteints.

## Mises à jour des logiciels et antivirus

L'ARPP veille à effectuer régulièrement les mises à jour du système et des logiciels utilisés. Lors de la configuration de nouveaux logiciels, la mise à jour automatique de la sécurité doit être cochée. Le système est régulièrement contrôlé à l'aide d'un antivirus.

## Back up

La sauvegarde automatique des données sur un serveur (ou à défaut un disque dur externe à garder en lieu sûr) est utilisée. Les documents sont en priorité enregistrés sur ce serveur et aucun document contenant des données personnelles n'est enregistré sur le bureau d'un ordinateur (et donc hors serveur et protection adéquate).

Les clouds (espace de stockage de données sur le web) sont proscrits car ils sont sujets au piratage. Une exception peut cependant être faite, avec l'accord de la direction, pour les clouds hébergés en Europe prouvant leur conformité au RGPD.

## Sécurisez le Wi-Fi

L'accès au Wi-Fi est sécurisé, notamment via un mot de passe différent de celui repris sur le routeur.

La fonction pare-feu est activée sur tous les ordinateurs. L'antivirus et pare-feu sont régulièrement contrôlés et mis à jour.

# Politique de sécurité de l'Association pour la Psychothérapie Psychanalytique.

Remarque : par travailleurs, il faut entendre : membres, salariés, indépendants, stagiaires et bénévoles / document à communiquer aux travailleurs et aux sous-traitants

## Le contrôle des messageries

L'ARPP applique des règles de sécurité en matière de messagerie. Le compte est régulièrement vérifié contre le piratage. Les pièces jointes d'expéditeurs inconnus et/ou douteux ne sont ni ouvertes ni téléchargées. L'ouverture automatique des téléchargement est désactivée. L'aval de la direction doit systématiquement être demandé pour le téléchargement de logiciels.

## Le cryptage des données

Les données collectées doivent être cryptées via un logiciel, particulièrement lorsqu'elles font l'objet d'un transfert. Les documents stockés sur le serveur sont cryptés.

## La destruction des données

Toute destruction de documents contenant des données personnelles doit se faire à l'aide d'une déchiqueteuse. Tout dossier/fichier informatique contenant des données personnelles doit être supprimé dans la corbeille et celle-ci doit être vidée systématiquement après chaque destruction de documents.

## La sécurité des accès physiques

L'accès physique aux dossiers tant papier qu'informatisés est limité au membre ou collaborateur qui en a légitimement l'accès, de par sa profession ou de par sa fonction, de part son adhésion. La configuration des espaces ne doit pas permettre un accès aisé au matériel informatique et/ou aux dossiers papier.

Les règles de sécurité générales s'appliquent, telles que la fermeture à clé et l'installation d'un système d'alarme. De plus, les armoires contenant des données personnelles des bénéficiaires et des travailleurs sont fermées à clés.

## La vérification des sous-traitants

L'Arpp s'assure que tout sous-traitant avec qui elle travaille soit en conformité avec les règles énoncées au RGPD. Pour ce faire, elle signe un contrat de sous-traitance qui indique que le sous-traitant s'engage à mettre en œuvre les mesures de sécurité adéquates.

## Règle en matière de fuite des données

En cas de perte, fuite ou envoi involontaire de données, le référent interne sur le RGPD notifie la fuite de données à l'Autorité de Protection des Données le plus rapidement après constat. Si les données perdues peuvent nuire gravement à la personne, celle-ci est informée. Il lui est décrit, en termes clairs et simples, la nature de la violation de données à caractère personnel. La violation est alors décrite au registre d'Activité de Traitement et un protocole de sécurité est mis en place pour prévenir sa répétition.

## Exercice des droits de la personne concernée

Toute personne physique est en droit de demander la rectification, l'effacement, l'accès, l'inventaire de ses données. Pour garantir sa sécurité, la personne doit prouver son identité en présentant sa carte d'identité. L'ARPP est dans l'obligation de s'exécuter, lorsque celle-ci est légitime et non régie par une

Remarque : par travailleurs, il faut entendre : membres, salariés, indépendants, stagiaires et bénévoles / document à communiquer aux travailleurs et aux sous-traitants

règlementation/loi. Dans tous les cas – légitime ou non –, l'ARPP répond à la demande, par écrit, afin de confirmer à la personne physique, l'exécution de ses droits ou la limite de ceux-ci en regard de la législation.

Toute demande d'effacement de données doit être exécutée (si légitime) dans les trente jours suivant la demande. Tout retrait de consentement est lui actif immédiatement.