Politique de signature électronique

Souscription dématérialisée à distance

Application « Demande d'adhésion en ligne SENOIS»

Définitions

Acte dématérialisé
Tout document proposé à l'Adhérent par voie dématérialisée tels que demande d'adhésion, document de gestion, fiche d'information précontractuelle, etc.

Adhérent
Personne physique manifestant son consentement sur le contrat auquel il demande d'adhérer en ligne via le portail web de l'Organisme Assureur.

Authentification
Processus permettant de vérifier l'identité déclarée d'une personne ou de toute autre entité, ou de garantir l'origine de données reçues.

Autorité d'archivage
Autorité chargée de procéder l'archivage des adhésions signées.

Autorité d'horodatage
Autorité chargée de procéder à l'horodatage.

Autorité de certification
Autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer des certificats.

Certificat
Clé publique de PANACEA, concaténée à d'autres informations rendues infalsifiables par signature avec la clé privée de l'Autorité de certification qui l'a délivré.

Certificat d'AC
Certificat d'une Autorité de certification.

Comité d'Approbation
Le Comité d'Approbation est composé de la Direction Juridique, de la Direction Commerciale et de la Direction des Systèmes d'Information du GIE GPS auquel les Organismes Assureurs sont membres.

Déclaration des pratiques de certification
Déclaration des pratiques mises en œuvre par une Autorité de certification pour émettre et gérer des Certificats.

Données d'activation
Données privées associées à un porteur permettant d'initialiser ses éléments secrets.

Hébergeur
Personne Morale spécialisée dans les prestations d'hébergement.

Infrastructure de gestion de Certificats
Ensemble de composantes fournissant des services de gestion de clés et de certificats au profit d'une communauté d'utilisateurs.

Liste de Certificats Révoqués
Liste contenant les identifiants des Certificats révoqués ou invalides.

Organisme Assureur

Tout Organisme Assureur proposant une signature dématérialisée de l'acte. De manière générale, Organisme Assureur de la garantie souscrite (AGMF Prévoyance ; GPM Assurance SA ; PANACEA) ; ou Mutuelle de livre 3 adhérente à AGMF Prévoyance

Pack SENOIS
Offre à destination des étudiants et internes de médecine permettant leur couverture en Responsabilité Civile Professionnelle (hors remplacement en libéral) et en cas d'impossibilité de poursuivre leur cursus. Elle leur permet également de bénéficier de services d'action sociale.

Plate-forme
La Plate-forme assure la transmission des informations d'identité nécessaires à la demande de Certificats vers l'Autorité de certification, la préparation des informations et la transmission du document PDF et la certification électronique par l'Organisme Assureur de l'Acte dématérialisé PDF signé électroniquement par l'Adhérent.

Politique de certification
Ensemble de règles relative à l'applicabilité d'un certificat à une communauté et / ou à une classe d'applications ayant des besoins de sécurité communs.

Portail web de l'Organisme Assureur.
Site web de l'Organisme Assureur permettant à l'Adhérent de souscrire en ligne à des Actes dématérialisés

Signature électronique.
En apposant sa signature, l'Adhérent s'identifie, confirme l'exactitude des éléments indiqués. La signature est donc la manifestation du consentement de l'Adhérent et ce conformément aux dispositions de l'article 1316-4 du Code civil

1. Objet du document

L'Organisme Assureur propose à ses Adhérents de dématérialiser le processus de demande d'adhésion en leur permettant de remplir les formulaires d'adhésion et de recueillir leur consentement par voie dématérialisée à distance.

La demande d'adhésion dématérialisée permet à l'Adhérent de signer électroniquement des Actes dématérialisés. L'Adhérent est conscient et informé qu'il s'agit uniquement et seulement d'une demande d'adhésion. Le contrat étant conclu dès la signature du Bulletin d'Adhésion par l'Adhérent, dans les conditions prévues aux conditions contractuelles régissant la garantie.

Le présent document a pour objet de décrire les conditions de création et de validation d'une Signature électronique dans le cadre des opérations de demande d'adhésion et de gestion des Actes dématérialisés.

L'objet de ce document « Politique de Signature électronique » est ainsi de décrire notamment :

- les conditions dans lesquelles sont réalisées, traitées, conservées ces Certificats électroniques ;
- les conditions et contexte dans lesquels ces Certificats électroniques seront ultérieurement consultables et vérifiables

Ces Actes dématérialisés signés par les Adhérents sont ensuite horodatés et conservés par l'Organisme Assureur. Ces Actes dématérialisés sont vérifiables et lisibles par les Adhérents au format PDF.

Ce document est destiné aux :
- Adhérents afin d'assurer la transparence des opérations de demande d'adhésion par Actes dématérialisés ;
- éventuels destinataires ultérieurs de ces Actes dématérialisés, ayant besoin d'en connaître.

La présente Politique de Signature électronique concerne les Adhérents (signataires d'Actes dématérialisés).

La structure de ce document est conforme aux documents normatifs suivants :

- *ETSI TR 102 041 V1.1.1 (2002-02) : Signature Policies Report*
- *RFC 3125 - Electronic Signature Policies*

Cette « Politique de Signature électronique » est accessible au format PDF.

2. Politique de signature électronique

2.1. Champ d'application

La présente Politique de Signature électronique est applicable à l'Acte dématérialisé (bulletin d'adhésion) signé électroniquement par l'Adhérent et l'Autorité de Certification. Les échanges électroniques sont réalisés par l'intermédiaire du Portail web de l'Organisme Assureur et d'une Plate-forme.

2.2. Validation de la Politique

Avant toute publication officielle, la Politique est validée par le Comité d'Approbation.

2.3. Processus

Dans le cadre de la souscription dématérialisée, la présente Politique est accessible préalablement à toute souscription, à l'adresse suivante :

http://www.gpm.fr/images/juridique/1.3.6.1.4.1.40706.1.6.1 PA v01.pdf

Dans le cadre de la demande d'adhésion, une fiche d'information de la garantie d'assurance à laquelle l'Adhérent demande de souscrire de façon dématérialisée est accessible préalablement à cette dernière.

L'Adhérent peut renoncer à sa demande d'adhésion à l'Acte dématérialisé si la présente Politique ou la fiche d'information ne lui conviennent pas. De manière générale, l'Adhérent peut renoncer à tout moment au cours du déroulement du processus à Adhérer

La demande d'adhésion de l'Adhérent s'effectue selon le formalisme suivant :

- L'Adhérent renseigne en ligne, sur le Portail de Service GPM, l'ensemble des informations nécessaires à l'établissement et à la gestion de son adhésion au Pack SENOIS. Toutes les informations sont obligatoires.
  La demande d'adhésion est établie d'après les déclarations de l'Adhérent. Toute fausse déclaration intentionnelle entraine la nullité du contrat (article L.221-14 du Code de la mutualité et L.113-9 du code des assurances).
  Il est impératif de suivre les instructions mentionnées à chaque étape et notamment de renseigner tous les champs obligatoires et de valider les informations renseignées à chaque étape au moyen des boutons de validation prévus à cet effet.
  Tout au long du processus, l'Adhérent peut effectuer des corrections en revenant aux étapes antérieures ou renoncer à cette dernière.

- L'Adhérent est invité à prendre connaissance de l'ensemble des documents (fiches d'information, conditions contractuelles, politique de signature) constituant le contrat de souscription au Pack SENOIS et à cocher la case confirmant qu'il en a bien pris connaissance. Cette étape est obligatoire. Il est possible pour l'Adhérent de télécharger ou d'imprimer ces documents.

- L'Adhérent est invité à prendre connaissance et à accepter la présente Politique de Signature électronique. Cette étape est obligatoire. L'Adhérent peut ensuite procéder à la signature de sa souscription :
  - L'Adhérent prend connaissance des différents documents contractuels et vérifie que toutes les informations renseignées sont exactes, complètes et sincères
  - Il clique sur le bouton « Signer en ligne » qui génère l'envoi d'un SMS au numéro de portable qui aura été préalablement renseigné
  - L'Adhérent renseigne le code numérique reçu par SMS dans la zone prévue à cet effet.
  - Le bulletin d'adhésion signé s'affiche dans une nouvelle fenêtre du navigateur de l'Adhérent. Il est fortement conseillé à l'Adhérent de télécharger et de sauvegarder ce document.
  - Les certificats de signature apparaissent au-dessus du contrat ; l'Adhérent peut en prendre connaissance et vérifier l'identité des signataires et la validité des certificats utilisés, en cliquant sur l'icône du certificat et en déroulant chaque certificat au moyen de la flèche devant chacun des certificats.

A l'issue des différentes étapes ci-dessus énumérées, l'Adhérent est informé par l'Organisme Assureur que la souscription au Pack SENOIS a pris effet par l'affichage du certificat d'adhésion, sous la forme d'un fichier PDF. L'Adhérent a également la possibilité de le télécharger et/ou de l'imprimer directement. Un courrier électronique récapitulant l'Adhésion, accompagné du bulletin d'adhésion est également envoyé à l'Adhérent.

En cas d'interruption dans le processus de demande d'adhésion, l'Adhérent doit reprendre le processus depuis sa première étape.

Si des inexactitudes ou erreurs ne sont pas identifiées (ex.: fautes d'orthographe, mauvaise saisie, etc.) et ne bloquent pas la demande d'adhésion dématérialisée, elles pourront néanmoins être rectifiées ultérieurement auprès des Services de l'Organisme Assureur, par téléphone, fax ou e-mail.

2.4. Identification

La présente « Politique de signature - Souscription dématérialisée à distance» est identifiée, au sein du référentiel documentaire de l'Organisme Assureur, par un numéro d'identification unique, l'OID : 1.3.6.1.4.1.40706.1.6.1 PA v01.

Les signatures et certificats respectant la présente Politique, la référenceront en utilisant ce numéro d'identification unique « OID », accompagné de l'empreinte de ce document et de la mention de l'algorithme utilisé pour produire cette empreinte.

2.5. Composition du Comité d'Approbation

Le Comité d'Approbation est composé de la Direction Juridique, de la Direction Commerciale et de la Direction des Systèmes d'Information de l'Organisme Assureur. Ce dernier approuve la Politique de signature.

2.6. Processus de mise à jour

La mise à jour de la présente Politique peut avoir pour origine l'évolution du droit, la modification de l'état de l'art, l'apparition de nouveaux risques et de nouvelles mesures de sécurité ou des modifications dans le processus de signature.

La présente Politique est réexaminée périodiquement.

La validité d'une signature électronique est appréciée conformément à la Politique applicable au moment de ladite signature.

Toutes les versions des Politiques et leur durée respective de validité sont donc conservées par l'Organisme Assureur et accessibles sur demande.

Après mise à jour, la Politique révisée est mise en ligne à l'adresse indiquée *supra*.

La publication d'une nouvelle version de la Politique de Signature consiste à archiver la version précédente et à mettre en ligne les éléments suivants :

- document au format PDF incluant,
  - l'OID associé,
  - son horodatage électronique,
  - la date et heure exacte d'entrée en vigueur.

2.7. Entrée en vigueur de la nouvelle version et période de validité

La nouvelle version de la Politique de signature entre en vigueur dès sa publication.

2.8. Cohérence de la documentation

Le Comité d'Approbation s'assure de la cohérence du référentiel documentaire dont fait partie la présente Politique de signature.

3. Acteurs et rôles

3.1. Les acteurs

Les acteurs concernés par le processus de création et de vérification de la signature électronique sont les suivants:

- l'Adhérent ;
- L'Organisme Assureur
- L'Autorité de Certification, Autorité d'Horodatage, Autorité d'Archivage, hébergeur sont des prestataires de confiance en charge des prestations de certification, d'horodatage, d'archivage ainsi que de l'hébergement de la plate-forme.

3.2. L'Adhérent

L'Adhérent s'engage à avoir au moment de la réalisation de sa demande d'Adhésion dématérialisée l'intégralité des informations à sa disposition ainsi que son téléphone portable sur lequel sera envoyé un SMS.
L'identité de cette personne physique est garantie par l'envoi d'un code par SMS au numéro renseigné lors de la demande d'Adhésion et renseigné par l'Adhérent sur la Plateforme de signature électronique

Le rôle de l'Adhérent est de vérifier que les informations contenues sur le document à signer sont exactes avant de donner son consentement et de signer électroniquement le document depuis la Plateforme de signature électronique de l'Organisme Assureur.

A l'occasion de la demande d'adhésion et de la souscription dématérialisée, l'Adhérent :

- respecte les règles de fonctionnement concernant les étapes de signature ;
- reste à proximité du terminal par lequel il signe électroniquement le document jusqu'à la fin du processus de souscription.

Les informations communiquées par l'Adhérent doivent être en cours de validité à la date de la demande d'adhésion dématérialisée et ce dernier certifie leur exactitude.

3.3. L'Organisme Assureur

3.3.1. *Gestion du processus de certification et de signature électronique*

L'Organisme Assureur et ses prestataires reconnus sur le marché, hébergent et maintiennent le système informatique, conformément à l'état de l'art stable et actuel.

3.3.2. Sécurité du processus de certification et de signature électronique

L'Organisme Assureur met en œuvre les moyens nécessaires, conformément à l'état de l'art stable et actuel, pour assurer la protection du processus de certification et de signature électronique. Les mesures prises concernent :

- l'hébergement sécurisé des infrastructures (protection physique, protection logique, alimentation secourue, détection et protection incendie, etc.) ;
- la restriction des accès logiques aux équipements ;
- la protection réseaux en assurant une authentification forte et la confidentialité des échanges d'informations ;
- la sensibilisation et le suivi des procédures dans le processus de signature.

3.3.3. Journalisation

L'Organisme Assureur assure une traçabilité et une conservation des traces relatives :

- aux différents échanges sur les réseaux et systèmes d'informations ;
- aux traitements des données échangés.

L'Organisme Assureur s'assure que les éléments constituant la signature électronique sont conservés pendant la durée prévue aux conditions contractuelles qui lui sont applicables à l'Acte dématérialisé auquel l'Adhérent a souscrit.

3.3.4. Type de certificat utilisé

L'Organisme Assureur utilise un certificat délivré par l'Autorité de certification CERTINOMIS. Ce certificat est émis conformément à la politique de certification Cachet Serveur, R.G.S. 1 étoile (OID : 1.2.250.1.86.2.2.1.22.1).

3.3.5. Protection du support de certificat

L'Organisme Assureur prend toutes mesures nécessaires pour protéger l'accès à son certificat et aux données secrètes associées, notamment le support qui lui a été remis (carte à puce, clé USB) et le code PIN associé.
L'Organisme Assureur se conforme à l'usage décrit dans « Conditions générales d'utilisation de CERTINOMIS». À ce titre, le certificat électronique est stocké sur un dispositif cryptographique qui doit être qualifié au minimum au niveau FIPS 140-2 Level 2 ou CWA 14169 (SSCD), et être conforme aux exigences du chapitre 12.1 de la politique de certification CERTINOMIS citée en 3.3.2.3 du présent document.
L'Organisme Assureur s'engage à protéger l'accès à son certificat électronique, à ne pas communiquer son code PIN ou ses mots de passe associés, excepté pour ses préposés ayant besoin d'en connaître.

3.3.6. Révocation du certificat

L'Organisme Assureur s'engage à demander la révocation de son certificat de signature en cas de perte, de vol, de compromission ou de simple suspicion de compromission de sa clé privée et se conformer ainsi aux « Conditions générales d'utilisation des certificats » de l'Autorité de certification CERTINOMIS.

3.3.7. Mise à jour des données utilisées

Certaines données, notamment les listes de révocations, ne peuvent être mises à jour en temps réel et il s'écoule plusieurs heures (24 heures au maximum) avant la publication de ces données par l'Autorité de Certification.
Dans ces conditions, il se peut qu'une signature électronique soit déclarée valide si elle est réalisée entre le moment où le certificat a été révoqué et le moment où sa révocation a été publiée par l'Autorité de Certification et prise en compte par l'Organisme Assureur
L'Organisme Assureur ne peut être alors tenue responsable de cet état de fait considérant cette « période de caution » inhérente à ce type de système.

3.3.8. Vérification de signature électronique

L'Organisme Assureur est en capacité d'effectuer une vérification de la qualité de la signature électronique préalablement à l'archivage de l'Acte dématérialisé auquel l'Adhérent a souscrit.

Pour la vérification de la signature électronique apposée sur les Actes dématérialisés, l'Organisme Assureur utilise les données à sa disposition, notamment les données publiques relatives au certificat de l'Organisme Assureur, telles que les listes de révocations.

Les Actes dématérialisés signés font l'objet d'un horodatage permettant :

- de s'assurer de la traçabilité des informations de date et heure de signature de ces Actes dématérialisés;
- de déterminer la liste de révocation à utiliser pour vérifier la validité de la demande d'adhésion dématérialisée.

L'arrêt de la validation empêche temporairement l'archivage électronique de l'Acte dématérialisé mais n'impacte en rien la validité de cet Acte, une fois horodaté.
L'Organisme Assureur *s'assure de mettre en œuvre les procédures et dispositifs techniques permettant de lancer une nouvelle vérification de l'Acte dématérialisé lorsque ce service technique sera de nouveau disponible ; cette relance est automatique tant que le service est indisponible.*

3.3.9. Responsabilité

L'Organisme Assureur ne pourra être tenue responsable des retards et conséquences dommageables dus à des événements qui ne lui sont pas attribuables ou qui résulteraient du fait de l'Adhérent, notamment en cas d'utilisation d'éléments inexacts ou incomplets mis à disposition par l'Adhérent.

L'Organisme Assureur ne pourra être tenue responsable des retards et conséquences dommageables dus à des cas de force majeure.

La responsabilité de l'Organisme Assureur ne peut être engagée au titre d'un dommage indirect.

La responsabilité totale de l'Organisme Assureur, sur la base d'une faute dûment prouvée, est limitée toutes causes et tous sinistres confondus, et ce quel que soit le fondement juridique de la réclamation et la procédure employée pour la faire aboutir, au montant de la prime moyenne de la garantie Panacéa de 200 euros ,.

L'action en réparation devra être engagée dans l'année suivant la survenance de l'événement dommageable.

L'Adhérent s'oblige à prendre toutes mesures, dont notamment des sauvegardes, pour éviter qu'un dommage quelconque ne résulte pour lui d'une éventuelle atteinte aux fichiers, mémoires, documents ou tous autres éléments qu'il aurait pu confier dans le cadre de souscription dématérialisée.

L'Organisme Assureur ne saurait être tenu d'indemniser l'Adhérent du fait de la destruction totale ou partielle de ses données ou fichiers qu'il appartient à l'Adhérent de sauvegarder.

L'Adhérent est responsable de l'exactitude et de la sincérité des données transmises, ainsi que de l'envoi des documents nécessaires à la complétude de la demande d'adhésion.

3.3.10. Assistance aux Adhérents

Les Adhérents peuvent signaler tout dysfonctionnement à l'adresse suivante : souscriptiondirecte@gpm.fr

4. Signature électronique et vérification

4.1. Caractéristiques du serveur de signature

Le serveur utilisé pour produire la signature électronique de l'Adhérent est un serveur hébergé chez un Docapost. Le serveur du prestataire envoie une requête pour effectuer la signature électronique mais la production de la signature est générée par Docapost.

4.2. Données signées par l'Adhérent

La signature électronique de l'Adhérent est apposée sur l'Acte dématérialisé auquel souscrit l'Adhérent dans sa forme définitive, c'est-à-dire après production par le système d'information de l'Organisme Assureur du document PDF exploitable par l'Adhérent et par les services internes de l'Organisme Assureur..

4.3. Opération de signature

L'opération de signature électronique est effectuée de façon automatique par le serveur de l'Organisme Assureur dès réception des Actes dématérialisés à signer. Cette opération de signature est effectuée après validation du paiement en ligne réalisé par l'Adhérent .L'Organisme Assureur ne saurait s'engager sur des délais impératifs, notamment compte tenu du fait que la réception des Actes dématérialisés est soumise aux réseaux de télécommunications.

4.4. Type de signature

Les Certificats électroniques apposées par les représentants des établissements assujettis sont de types enveloppés.

4.5. Norme de certificat

Les signatures respectent la norme PAdES (ETSI TS 101 733).

Conformément à cette norme, les propriétés signées (SignedProperties / SignedSignatureProperties) contiennent les éléments suivants :

- le certificat du signataire (SigningCertificate) ;
- la date et l'heure de signature (SigningTime) ;
- l'identifiant de l'émetteur (IssuerSerial) ;
- lieu de la signature (SignatureProductionPlace).

Une fois signé :

- le fichier signé est immédiatement horodaté et complété par l'usage du profil de signature PAdES-T, intégrant la signature électronique et un jeton d'horodatage, permettant de déterminer la date et l'heure de la signature ;
- il ne fait ensuite plus l'objet d'aucun transcodage, et transite dans le système d'information de l'Organisme Assureur sous la forme d'un flux binaire, avant d'être stocké dans le SI de l'Organisme Assureur.

4.6. Algorithmes utilisables pour la signature

4.6.1. Algorithme de condensation

L'algorithme de condensation supporté est SHA-256.

4.6.2. Algorithme de chiffrement

L'algorithme de chiffrement à utiliser est RSA Encryption.

4.6.3. Mise en forme canonique

Sans objet.

4.7. Horodatage de la signature

Le jeton d'horodatage intégré au fichier signé est conforme à la norme RFC3161.
Il est produit par l'Autorité d'Horodatage DOCAPOST selon sa Politique d'horodatage identifiée par l'OID 1.2.250.1.229.1.3.

4.8. Conditions pour valider le fichier signé

Un fichier signé et horodaté est considéré comme valide par l'Organisme Assureur à l'issue de la réception de l'acquittement produit par le Système d'information de l'Organisme Assureur utilisé pour conserver ces fichiers, garantissant ainsi que ces fichiers seront bien conservés de façon sécurisée et exploitables ultérieurement.

4.9. Vérification de la signature

À l'issue de l'opération de signature électronique, l'Adhérent est informé que l'Organisme Assureur est en capacité de réaliser des opérations de vérifications de ces signatures électroniques.

La vérification de la signature électronique porte sur :

- la vérification du respect de la norme de signature ;
- la vérification de l'appartenance du certificat du signataire à la famille de certificat citée en 3.3.4 du présent document. ;
- la vérification du certificat de l'Organisme Assureur et de tous les certificats de la chaîne de certification:
    - validité temporelle,
    - statut,
- la vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue ;

  la vérification du Certificat de l'Organisme Assureur et de la signature électronique apposés sur le fichier

5. Contrôle de conformité

5.1. Objectif du contrôle

Le procédé de Certificat s'appuie sur un ensemble d'exigences et de règles de sécurité devant favoriser la confiance. L'Organisme Assureur effectuera donc en ce sens des contrôles réguliers de conformité et de bon fonctionnement permettant de valider que le Certificat est conforme aux politiques de signature et de certification.

5.2. Fréquence du contrôle de conformité

L'Organisme Assureur procède annuellement à un contrôle de conformité.

5.3. Choix du contrôleur

Le contrôle est effectué à la demande de l'Organisme Assureur par une équipe d'auditeurs externes compétents en sécurité des systèmes d'information et indépendante.

5.4. Communication des résultats

Les résultats des audits de conformité contiennent des informations sensibles. Ils sont communiqués à un nombre restreint de personnes dans les entités concernés par l'audit en fonction des résultats.

5.5. Plan d'action

À l'issue d'un contrôle de conformité, les auditeurs externes rendent un avis et proposent un plan d'action afin de corriger le cas échéant les non-conformités détectées. Le plan d'action est communiqué aux seules personnes directement concernées.

6. Confidentialité

Les informations suivantes sont considérées comme confidentielles :

- les clés privées associées aux certificats ;
- le dossier de demande d'adhésion de l'Adhérent;
- le dossier d'archivage de tous les éléments électroniques de l'Adhérent;
- les journaux d'évènements de la plate-forme de médiation de signature ;
- les procédures internes ;
- les rapports d'audits.

Les informations énumérées ci-dessus ne sont accessibles qu'aux personnes habilitées par l'Organisme Assureur et ayant besoin d'en connaître.

7. Dispositions juridiques

7.1. Loi applicable

Le procédé de signature électronique est soumis à la législation et la réglementation française en vigueur.

7.2. Réclamation - Médiation

Toute information complémentaire ou réponse à une réclamation concernant l'application de l'Acte dématérialisé auquel l'Adhérent a demandé l'adhésion est fournie par le Département des Services Adhérents de l'Organisme Assureur au siège social selon les modalités relatives à toute réclamation ou médiation décrites dans les conditions contractuelles applicables à l'Adhérent.

7.3. Attribution de compétence

Tout différend né de l'interprétation ou de l'exécution de la Politique de signature relèvera de la compétence expresse du Tribunal du ressort de la Cour d'appel de Paris, nonobstant pluralité de défendeurs ou appel en garantie, y compris pour les procédures d'urgence ou les procédures conservatoires, en référé ou par requête.

7.4. Propriété intellectuelle

Les Adhérents, ne disposent pas des droits de propriété intellectuelle sur les éléments composant le service de signature, dont l'Organisme Assureur est titulaire.

7.5. Protection des données personnelles

7.5.1. Informations à caractère personnel

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

7.5.2. Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel sont réalisés dans le strict respect de la loi dite « Informatique et Libertés » du 6 janvier 1978.

Le traitement automatisé des données à caractère personnel, réalisé au titre de la présente Politique de signature, a fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Conformément à l'article 32 de la loi Informatique et Libertés, les Adhérents sont informés que les données à caractère personnel qu'ils communiquent pourront être transmises et exploitées par l'Organisme Assureur et ses différents partenaires contractuels.

Les Adhérents sont informés qu'ils bénéficient d'un droit d'accès et de rectification aux données qui les concernent, qu'ils peuvent exercer en s'adressant à :

Groupe Pasteur Mutualité
Direction des Systèmes d'Information
Service Correspondant Informatique et Libertés
34, bd de Courcelles, 75809 Paris Cedex 17

Les Adhérents sont également informés qu'ils bénéficient d'un droit d'opposition, pour motif légitime, au traitement des données qui les concernent, qu'ils peuvent exercer en s'adressant à l'adresse ci-dessus.

7.6. Droit de renonciation ou de rétractation

L'Adhérent dispose d'un droit de rétractation ou de renonciation. Ce droit de rétractation doit être exercé obligatoirement par lettre recommandée avec demande d'avis de réception selon les modalités relatives au droit de renonciation ou de rétractation décrites aux conditions contractuelles applicables à l'Adhérent.