ASSUR+CONSEILS

VOTRE ASSUREUR DE PROXIMITÉ

CONTEXTE

En France, la protection des données personnelles est encadrée par la loi du 6 janvier 1978 dite « Informatique et libertés ».

Cette loi a été modifiée le 20 juin 2018 pour l'adapter aux dispositions du Règlement général sur la protection des données (RGPD), applicable partout en Europe depuis le 25 mai 2018.

L'organisme régulateur de contrôle et de sanctions en France est la commission nationale informatique et libertés dite CNIL.

Nous traitons des données personnelles au sens du RGPD.

L'article 4 du RGPD donne une définition large des données personnelles.

Il s'agit ainsi de toute information se rapportant à une personne physique identifiée ou identifiable "tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale."

Les moyens d'identifier une personne sont multiples.

Il peut s'agir de moyens d'identification :

- *directs (exemple : nom et prénom) ;*
- *ou indirects (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).*

L'identification d'une personne physique peut être réalisée :

- *à partir d'une seule donnée (exemple : nom) ;*
- *à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association).*

Les données personnelles concernent seulement les personnes physiques.
En effet, les coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1@email.fr ») ne sont pas, en principe, des données personnelles.
Les données des personnes morales ne relèvent ainsi pas de la protection du RGPD.
Certaines de ces données sont dites sensibles :

- *Des données relatives à la santé de la personne assurée : Données liées à l'état de santé de la personne, Numéro de sécurité sociale,*
- *Des données relatives aux infractions routières.*

Les personnes dont les données sont traitées ont des droits. Les entreprises sont responsables de la protection des droits des personnes en matière de protection des données personnelles.

Ces droits, retranscrits dans l'image ci-dessous, sont de plusieurs natures.

Le rôle du responsable du traitement qui est M. PAYMAL GHISLAIN au sein de notre structure est de sécuriser le traitement des données personnelles.

Comment collecter les données personnelles ?

La collecte doit être minimisée.
L'article 5.1.c) du RGPD définit le principe de minimisation des données de la manière suivante : Les données à caractère personnel doivent être collectées pour des finalités adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Nous ne devons ainsi uniquement traiter les données personnelles dont nous avons besoin afin d'atteindre l'objectif initial :

- Souscription d'un contrat,
- Gestion des contrats et des sinistres,
- LCB-FT

De même, L'objectif final de la collecte doit être strictement respecté. Les données de notre fichier ne doivent servir que pour les finalités définies au moment de leur collecte.
A noter : nous recueillons, après avoir informé le client des finalités de la collecte sur notre site internet et sur les recueils de besoins, son consentement actif.

Il est à noter que les données de santé sont des éléments dits sensibles. Nous devons ainsi :

- laisser la personne remplir le questionnaire de santé seule. En pratique, vous devez donc soit lui proposer de remplir le questionnaire à son domicile, soit lui laisser un endroit isolé dans lequel elle pourra le remplir.
    - Si la personne remplit le questionnaire chez elle, attention cependant à la transmission de ce questionnaire qui ne doit pas se faire par mail. En principe en effet, cette dernière doit envoyer le questionnaire soit directement à la société d'assurance, soit vous l'envoyer dans une enveloppe cachetée identifiée comme contenant des données de santé, à transmettre au médecin conseil de la société d'assurance.

- Si la personne vous envoie quand même ces données par mail, ne le transférer par à la société d'assurance par mail, sauf si cette dernière a mis en place un service spécifique, avec une adresse mail permettant de transmettre ce genre de données.
- Dans tous les cas, ne conservez aucun questionnaire de santé que ce soit en format papier ou numérique.

Comment conserver les données personnelles ?

Quelles données conserver ?
Les données à conserver doivent respecter le principe de minimisation. En ce sens, ces données doivent être :

- adéquates : sont-elles encore actuelles ?
- pertinentes et limitées au regard des finalités pour lesquelles elles sont traitées : sont-elles nécessaire au regard de la finalité.

Les données à conserver doivent ainsi être sélectionnées en fonction de la nature de la finalité qui peut en assurance être liée à :

- la vie du contrat d'assurance,
- la protection de nos intérêts judiciaires en cas de mise en cause de votre RC par le client ou la société d'assurance.

Type de contrat	Durée maximale
Contrat en cours / non résilié	Conservation
Contrat IARD / de personnes résilié / échu	2 ans après résiliation / terme
Contrat dommage ouvrage / responsabilité civile décennale	12 ans après la souscription du contrat

Pour rappel, notre archivage est organisé de telle sorte à ce que les contrats résiliés et données des prospects n'ayant pas donné suite à nos propositions puissent être isolées par années. Ces données seront détruites de notre système informatique grâce à la mise en place de logiciels d'effacement sécurisé qui nettoient les données des appareils ou la démagnétisation du disque dur.

Les éventuelles données en format papier seront quant à elles confiées à des entreprises spécialisées dans la destruction. Une déchiqueteuse est par ailleurs disponible au sein de l'agence. Elle devra être utilisée et conservée en parfait état de marche.

Comment sécuriser les données personnelles traitées ?

Qu'est-ce que la violation des données personnelles ?

L'article 4.12) du RGPD définit une violation de données à caractère personnel comme : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.
Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre :

- *l'intégrité,*
- *la confidentialité*
- *ou la disponibilité de données personnelles.*

Le RGPD responsabilise les entreprises face aux risques de violation et impose de ce fait à ces dernières de sécuriser les données.

Informations juridiques du cabinet

Sécuriser les données implique de prendre des précautions pour préserver la sécurité des données contre les risques de violation.

Les principales mesures que nous vous demandons de prendre sont NOTAMMENT les suivantes :

- Respecter la confidentialité des données de nos prospects et clients en leur permettant notamment de pouvoir s'exprimer en toute confidentialité dans nos locaux et en respectant de ce fait la réception de notre clientèle dans les espaces privatifs,
- Ne divulguer même sous couvert de l'anonymat aucune donnée personnelle pouvant être recoupée et donc utilisée contre notre clientèle,
- Ne pas transmettre vos mots de passe à vos collègues, y compris par praticité,
- Ne pas garder de données clients / prospects sur vos postes individuels et utiliser les serveurs externes de sauvegarde mis à votre disposition,
- Sécuriser vos postes de travail en n'allant pas sur des sites web non utiles à votre activité et en téléchargeant pas de pièce jointe douteuse,
- Conserver vos documents et les données personnelles de nos clients dans les armoires fermées à clés prévues à cet effet,
- Ranger vos bureaux,
- Veiller à prévenir les risques d'incendie et de dégâts des eaux en adoptant une conduite responsable.

En cas de violation

Il est prévu le processus suivant :

1- **Notifier l'incident à la CNIL dans les 72 heures par le biais du téléservice sécurisé dédié**
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
La notification doit contenir a minima les éléments suivants :

- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les conséquences probables de la violation ;
- les coordonnées de la personne à contacter (DPO ou autre) ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

2- **Avertir les parties prenantes**

a) Les personnes physiques et morales concernées par le risque de violation des données *en cas de risque élevé d'atteinte à leurs droits et libertés*

L'appréciation se fait au cas par cas en fonction des éléments suivants :

- Type de violation
- Sensibilité et volume des données concernées
- Facilité d'identifier les personnes touchées
- Conséquences possibles sur les personnes

b) Les fournisseurs des contrats de ces personnes selon les délais et les modalités prévues dans les conventions de courtage. A vérifier par le responsable du traitement des données à l'aide de son délégué régional si besoin

3- Actualiser le registre de violations des données

Ce dernier contient les éléments suivants :

- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les conséquences probables de la violation ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- le cas échéant, la justification de l'absence de notification auprès de la CNIL ou d'information aux personnes concernées

Informations juridiques du cabinet