Leto

ASSURANCE ET RGPD : QUELS ENJEUX ?

NOS CONSEILS

LETO. LEGAL

SOMMAIRE

LES POINTS CLÉS

Le RGPD a de lourdes conséquences pour le secteur de l'assurance. Le milieu de l'assurance traite directement les données personnelles, parfois même sensibles, de tout souscripteur.
Afin de comprendre les enjeux du RGPD en matière d'assurance, il convient de répondre à plusieurs questions.
Quels sont les acteurs ? En quoi le domaine de l'assurance est spécifique pour le traitement des données ? Quelles sont les priorités pour se mettre à jour ?

ASSURANCE : CHAMP D'APPLICATION DU RGPD

Des données particulières

Selon le RGPD, une donnée personnelle est une information se rapportant à une personne physique identifiée ou identifiable de façon directe ou indirecte (article 4 RGPD).

Or, beaucoup d'organismes, assureurs y compris, ont accès à un grand nombre de renseignements (coordonnées, âge, numéro de sécurité sociale, identifiant, etc.).

En matière d'assurance, la spécificité réside dans l'analyse poussée des différentes données de l'assuré : situation financière, santé, patrimoine, travail, etc. Cela permet un profilage pour prédire des comportements et établir une grille des risques.

Bien évidemment, ce profilage nécessite l'application d'une protection particulière prévue par le RGPD car il comporte un risque évident concernant les libertés des personnes visées.
Pour rappel, le profilage est un type de traitement de données personnelles automatisé, c'est-à-dire effectué par un algorithme, pour évaluer certains aspects personnels relatifs à une personne en vue de prédire un comportement (article 4 RGPD). Ce type de traitement est réglementé par l'article 22 RGPD.

Leto

Focus sur les données de santé

En fonction des services proposés par les assureurs, ces derniers ont inévitablement accès à des données de santé : complémentaire santé, prévoyance, assurance vie etc.

Il s'agit de données dites "sensibles" dont la collecte et l'utilisation ne sont autorisées qu'à certaines conditions, notamment :

- Lorsque la personne concernée a librement donné son consentement,
- Lorsque le traitement est nécessaire à l'exécution de contrat dans le champ de la protection sociale.

C'est sur le fondement de cette deuxième exception que les assureurs sont en droit de collecter et utiliser des données de santé. En effet, les contrats de complémentaires santé, prévoyance, assurance vie ou encore retraite correspondent à des contrats relevant de la protection sociale.

Leto

Responsable de traitement et sous-traitant : les acteurs de l’assurance

Le responsable de traitement est la personne morale qui définit les moyens et les finalités de traitement (article 4 RGPD).

Dans notre cas, il s’agit de comme le courtier ou la compagnie d’assurance.
Le sous-traitant quant à lui agit pour le compte du responsable de traitement et sur les instructions du responsable de traitement (article 4 RGPD).

Sont concernés les mandataires de la compagnie d’assurance, ses sous-traitants et tous les outils informatiques utilisés par la compagnie d’assurance.

ASSURANCE : IMPACTS DU RGPD

La sécurité des données et le domaine des assurances

Les compagnies d'assurances doivent s'assurer que les données qui leur sont confiées ne peuvent pas faire l'objet de vol, d'intrusion bien de modification par des tiers.

Pour assurer la protection de ces données, plusieurs mesures de sécurité peuvent être mises en œuvre :

- chiffrement des archives numériques
- utilisation de clés cryptographiques, politique de mot de passe conforme aux recommandations de la CNIL, etc.

La cybersécurité est donc l'une des composantes pour bénéficier d'un haut niveau de sécurisation.

Par ailleurs, en cas de fuite de données, il est indispensable de prévoir un protocole afin d'une part, de prévenir la CNIL et d'autre part, d'avertir les intéressés, étant entendu que tous ces événements sont à consigner.

Les droits des assurés

Information renforcée

Informer les assurés signifie qu'il faut effectuer un réel effort pour rendre l'information accessible et compréhensible. La CNIL recommande une approche à deux niveaux :

- **les informations essentielles classiques** : les types de données récoltées, l'identité et les coordonnées du DPO, les finalités du traitement, l'existence des droits, etc.
- **les informations complémentaires : la durée de conservation des données, les sous-traitants UE ou hors UE, l'existence ou non de profilage, etc.**

Les droits des assurés

Exercice des droits

Les assureurs doivent porter une attention particulière aux exercices des droits des personnes concernées par ces données.

À la moindre demande, le responsable de traitement doit répondre le plus rapidement possible et au plus tard, dans le délai d'un mois. Concernant les données de santé, le délai est de 8 jours !

Pour rappel, voici ceux que la personne concernée peut exercer :

- le droit d'accès ;
- le droit de rectification ;
- le droit d'opposition ;
- le droit à l'effacement ;
- le droit à la limitation ;
- le droit à la portabilité ;
- le droit à l'intervention humaine face à un profilage.

La durée de conservation des données

L'éternité n'existe pas en matière de conservation des données. On se réfère généralement à la durée pour la constatation, la défense ou l'exercice d'un droit en justice.

Par conséquent, on se réfère souvent au délai de prescription en justice, qui hors spécificité, est égale à 5 ans. Le délai de conservation des données peut alors s'indexer sur ce délai de 5 ans à compter de la collecte ou du dernier contact avec le prospect.

De plus, le Code des assurances prévoit des délais de prescription spécifiques pour certains contrats comme l'assurance vie qui bénéficie d'un délai de 30 ans à partir du décès de l'assuré pour les actions du bénéficiaire.

ASSURANCE et RGPD : MISE EN PLACE

Au regard des spécificités de ce domaine, nous vous conseillons de travailler sur les 5 priorités suivantes :

- La sécurité des données qui vous sont confiées. Les risques cyber existent : il convient de choisir une architecture informatique solide et de vous doter d'un logiciel qui traque les intrusions ;
- La désignation d'un DPO est fortement recommandée (voire obligatoire). Son rôle de chef d'orchestre est essentiel : il aura une vue intégrale sur les données gérées par l'ensemble des services ;
- La tenue d'un registre qui énumère le type de données collectées, l'utilisation qui en est faite, les bases légales, l'objectif de leur utilisation etc..
- L'exercice des droits : Il est nécessaire de prévoir un protocole spécifique pour répondre le plus rapidement possible au demandeur et procéder à l'effacement des données en interne si tel est l'objet de la demande ;
- Le choix d'un outil digital : suivre les informations à la main est chronophage et source d'erreurs. Il existe des logiciels tels que Leto qui automatise les nombreuses obligations imposées par le RGPD.

CONTROLES CNIL

La CNIL a utilisé son pouvoir de contrôles et de sanctions ces dernières années, notamment dans le secteur de l'assurance. Elle a effectué des contrôles autant sur place qu'en ligne. Voici quelques exemples d'entreprises contrôlées :

- **ALAN**
- **AMALFI SAS**
- **CNAM**
- **CNAM SEINE SAINT DENIS**
- **CNAM COTE D'OR**
- **COVERD**
- **LEOCARE**
- **LUKO COVER**
- **SHIFT TECHNOLOGY**
- **SOGESSUR**
- **AG2R LA MONDIALE**
- **ARTEX ASSURANCES**
- **EUROPASSISTANCE**
- **MALAKOFF MEDERIC MUTUELLE**
- **ALFA**
- **HUMANIS ASSURANCES**
- **SAMASSUR**

FAITES CONFIANCE À LETO

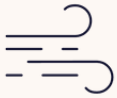
Comment mettre en œuvre le RGPD dans une entreprise de manière efficace ? Comment transformer cette contrainte réglementaire en opportunité de développement de son activité ?

C’est en partant de ces enjeux rencontrés dans leurs expériences entrepreneuriales que Benjamin et Édouard ont créé Leto.

Leto est une solution Saas dont l’ambition est d’automatiser la mise en conformité au RGPD et d’en faire une réalité opérationnelle au quotidien dans l’entreprise.

CAS CLIENTS

Leto accompagne une entreprise spécialisée dans l'IARD et l'intelligence artificielle pour gérer sa mise en conformité, sensibiliser ses équipes et prouver son respect du RGPD auprès de ses partenaires.



La crise climatique impacte fortement les métiers de l'assurance. Une entreprise spécialisée dans l'estimation de l'exposition au risque climatique des biens immobiliers fait confiance à Leto pour le pilotage de sa conformité au RGPD.

LETO VOUS PERMET DE

Gagner du temps au quotidien

Leto réalise et maintient automatiquement l'inventaire des types de données personnelles traitées par l'organisation et toute la documentation de conformité.

Raccourcir votre cycle de vente

Leto aide vos équipes (commerciale, compliance, etc.) à répondre aux audits et questionnaires conformité de vos prospects

Réduire votre risque réputationnel

Leto simplifie les procédures de demandes d'exercices de droits des citoyens (salariés, clients, candidats …),

Améliorer la maturité des équipes

Leto sensibilise l'ensemble vos collaborateurs à la protection des données personnelles grâce une technologie unique de microlearning ultra-personnalisé.

LETO.LEGAL

ENVIE D'EN SAVOIR DAVANTAGE ?

N'HÉSITEZ PAS À NOUS CONTACTER.

NOTRE E-MAIL :
contact@leto.legal

NOTRE SITE WEB :
leto.legal

NOTRE NEWSLETTER :
leto.legal/newsletter-rgpd

NOTRE CHAINE YOUTUBE :
youtube.com/@letolegal

NOS LIVRES BLANCS :
leto.legal/livre-blanc/rgpd