# POLITIQUE DE GESTION ET DE PROTECTION DES DONNEES PERSONNELLES

Version n° 2 du 01/01/2025

**Sommaire**

## PREAMBULE

La protection des données personnelles revêt une grande importance pour notre entreprise, eu égard aux conséquences dommageables pouvant résulter d'une atteinte, d'un détournement, ou plus généralement d'une utilisation frauduleuse de ces dernières pour les personnes auxquelles elles se rattachent.

Pour notre entreprise, soucieuse de protéger les intérêts de ses clients, prospects, mais aussi collaborateurs, il s'agit donc d'un sujet global impliquant le concours de l'ensemble des équipes et nécessitant notamment, pour chaque collaborateur, outre le respect et l'application des process internes dédiés, d'adopter un comportement prudent par rapport aux traitements des données ainsi qu'une approche constructive et pragmatique des process établis afin de pouvoir proposer de les renforcer, de les adapter ou bien encore de les faire évoluer lorsqu'il apparaît que ceux-ci sont (devenus) inadéquats ou insuffisants par rapport aux dispositions légales et réglementaires d'une part, mais également par rapport aux objectifs poursuivis d'autre part.

Le Règlement Général sur la Protection des Données UE 2016/679 du 27 avril 2016 (le « **RGPD** ») renforçant le dispositif légal national encadrant le traitement et la protection des données personnelles, crée de nouvelles obligations pour toute personne réalisant des traitements, automatisés ou non, de données à caractère personnel, dès lors que ceux-ci sont réalisés dans le cadre des activités d'un établissement situés sur le territoire de l'Union Européenne et/ou dès que les données concernent des ressortissants de l'Union Européenne, que les opérations de traitement aient lieu ou non sur le territoire de cette dernière.

Par conséquent, le RGPD s'applique à tout traitement de données personnelles que celles-ci concernent un prospect, un client, un collaborateur salarié et plus généralement toute personne physique identifiée ou identifiable grâce à ces données (les « **Personnes Concernées** »).

A l'instar d'autres réglementations impactant notre activité d'intermédiaire d'assurances (LCB/FT, solvabilité II…), la protection des données s'inscrit dans une logique de responsabilisation (*accountability*) des acteurs en application de laquelle notre entreprise doit adopter des mesures organisationnelles et opérationnelles internes, qu'elle estime adaptées et suffisantes notamment (i) au regard des objectifs de protection des intérêts des Personnes Concernées et (ii) des risques inhérents aux traitements qu'elle met en œuvre et encourus par ces dernières.

Ainsi, que notre entreprise agisse en qualité de Responsable du traitement des données (qu'elle collecte et traite dans le cadre du mandat qu'elle conclut avec ses clients), ou bien en tant que sous-traitant des compagnies avec lesquelles elle travaille (lorsqu'elle traite des données pour le compte de ces dernières dans le cadre de délégations conclues avec elles), celle-ci a décidé, d'ériger et d'appliquer une Politique de Gestion et de Protection des Données Personnelles, laquelle est composée du présent support et de ses annexes (la « **PGPD** »).

La PGPD regroupe l'ensemble des mesures organisationnelles, opérationnelles et informatiques internes élaborées par notre entreprise en vue d'encadrer son comportement ainsi que celui de ses collaborateurs en matière de protection des données personnelles. Elle est librement consultable en faisant la demande auprès du représentant du cabinet, Madame HAMEL Marie-Pascale par email à contact@galilee-finances.fr .

## I. DEFINITIONS UTILES

**Données à caractère personnel :**

Toute information se rapportant à une personne physique identifiée ou identifiable.

**Personne physique identifiable :**

Personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, 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.

**Traitement :**

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

**Pseudonymisation :**

Traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable

**Fichier :**

Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

**Responsable du traitement :**

Personne physique ou morale, l'autorité publique, ou tout autre organisme qui, seul ou conjointement avec d'autre(s), détermine les finalités et les moyens du traitement. Lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre

**Sous-traitant :**

Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

**Consentement :**

Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement

**Violation de données à caractère personnel :**

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

**Données concernant la santé :**

Données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

## II. MESURES ORGANISATIONNELLES INTERNES

### A. Désignation d'interlocutrices(teurs) dédiés(es) à la gestion et à la protection des données personnelles

En sa qualité de Gérant, Madame HAMEL Marie-Pascale agit en qualité de « **Représentant du responsable de traitement** » de notre entreprise. Elle est à ce titre, en matière de protection et de traitement des données, l'interlocuteur privilégié de l'Autorité de contrôle, des tiers et des clients pour toute question relative à la protection des données dans l'entreprise. Il peut, le cas échéant, déléguer une partie de sa mission au « **Délégué à la Protection des Données** » (« **DPO** »).

Notre entreprise n'étant pas tenue de désigner un DPO, pour toute question relative à l'application de la PGPD, ou plus généralement toute interrogation afférente à la protection des données, merci de prendre contact avec Madame HAMEL Marie-Pascale, gérante, et joignable par email à contact@galilee-finances.fr ou par courrier au 507 Rue des renards 76190 Sainte-Marie-des-Champs « **Référent(e) protection des données** » de notre entreprise.

La « Référent(e) protection et gestion des données », eu égard à la formation spécifique qu'elle a reçue, a pour mission d'informer et de conseiller les collaborateurs de notre entreprise quant aux problèmes relatifs à la protection et à la gestion des données d'une part et de contrôler la bonne application et applicabilité de la PGPD d'autre part, sous la responsabilité du Représentant du responsable de traitement.

### B. Mise en place d'un service dédié à la gestion des réclamations liées au traitement des données personnelles

Afin de permettre aux Personnes Concernées de pouvoir poser toute question relative à la protection de leurs données, d'exercer tout droit qu'elles détiennent sur ces dernières au titre de la réglementation applicable, ou bien encore d'introduire toute réclamation y afférente, notre entreprise a mis en place un service de réclamation dédié, lequel jouit des moyens appropriés à l'exercice de sa mission (le « **Service Réclamations des données** »).

Une réclamation au sens du présent paragraphe s'entend comme toute manifestation d'un mécontentement ou interrogation d'une personne concernée par les données que notre entreprise exploite dans le cadre de son activité relatif à l'exercice de l'un ou l'autre des droits qu'elle détient au titre de la réglementation applicable tels que notamment :

- le droit d'accès ;
- le droit de rectification ;
- le droit d'information ;
- le droit à l'effacement ;
- le droit à la limitation ;
- le droit à la portabilité ;
- le droit à l'opposition ;
- le doit d'introduire une réclamation.

Le Service Réclamations des données est composé des personnes suivantes :

Madame HAMEL Marie-Pascale, gérante du cabinet.

Le Service Réclamations des données peut être contacté par l'un ou l'autre des moyens suivants :

507 Rue des renards 76190 Sainte-Marie-des-Champs ou par email à reclamations@galilee-finances.fr

Conformément à la réglementation, le Service Réclamations des données doit répondre dans les meilleurs délais, et au maximum sous un (1) mois, à toute question ou réclamation posée par une Personne Concernée, après s'être assuré par tous moyens, en cas de doute, que son auteur et la Personne Concernée visée par la demande sont bien la même personne (notamment en lui demandant son adresse, sa date de naissance ou bien encore son deuxième prénom si la Personne Concernée en possède un).

Si le Service Réclamations des données ne donne pas suite à la demande formulée par la Personne Concernée, il informe celle-ci sans tarder et au plus tard dans un délai d'un (1) mois à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès de l'autorité de contrôle (la CNIL) et/ou de former un recours juridictionnel.

Le Service Réclamations des données n'exige aucun paiement supplémentaire pour répondre aux questions qui lui sont posées ou plus généralement pour traiter les réclamations qui lui sont adressées.

Toutefois, lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le Service Réclamations des données peut alors soit :

- Exiger le paiement de frais d'un montant maximum de 250 euros, lesquels doivent tenir compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées, soit ;
- refuser de donner suite à ces demandes.

En application du principe précité, l'entreprise pourra refuser de répondre ou demander à un client le paiement de frais spécifiques à la gestion d'une nouvelle demande déjà présentée et pour laquelle une réponse valable aura déjà été donnée, dès lors que cette demande sera :

- soit parfaitement injustifiée par rapport à la finalité des traitements pour lesquels la Personne Concernée a donné son consentement ;
- soit manifestement infondée ou de mauvaise foi ;
- soit présentée pour la seconde fois au cours du même mois.

Le Service Réclamations des données tient à jour un tableau de suivi des réclamations relatives aux données (distinct du tableau de suivi des réclamations clients), lequel doit être adressé au moins une fois par an au Référent protection des données.

En fonction du nombre de demandes et/ou réclamations, et au minimum 1 fois par an le Service Réclamations des données se réunit avec le Représentant du Responsable de traitement en vue de mettre en exergue les difficultés rencontrées au cours de la période écoulée et de proposer, le cas échéant, des mesures et actions correctives. Chacune de ces réunions doit faire l'objet d'un compte rendu précisant les personnes présentes, un résumé du contenu des échanges ainsi que la liste des décisions prises et des délais de mise en œuvre adoptés.

### C. Création d'un comité en charge du contrôle de l'application de la PGPD (le « Comité de contrôle »)

Le Comité de contrôle est en charge du contrôle de la bonne application et de l'applicabilité de la PGPD ainsi que de la réglementation applicable. Il est composé du Représentant du responsable de traitement et du Référent(e) protection et gestion des données.

Le Comité de contrôle est en charge de l'audit et du contrôle de l'ensemble des mesures internes mises en œuvre par notre entreprise au titre de la protection des données.

Tous les ans, le Comité de contrôle établit un contrôle de l'ensemble des mesures internes afin de voir si celles-ci ont été correctement appliquées au cours de la période considérée.

Pour ce faire, le Comité de contrôle doit, a minima :

- contrôler que la politique de restriction de l'accès aux données a été respectée, notamment en s'assurant que seules les personnes autorisées ont pu avoir accès aux données et/ou les modifier ;
- vérifier que l'ensemble des questions et réclamations adressées au Service Réclamations des données ont été traitées dans les délais et ont fait l'objet d'une mise à jour du tableau de suivi ;
- contrôler que le registre des activités de traitement est à jour ;
- s'assurer du respect du principe de minimisation des données, lequel impose à notre entreprise de ne pas traiter plus de données que nécessaire par rapport aux finalités de traitement que nous poursuivons ;
- auditer les mesures de protection internes des données et notamment informatiques afin de s'assurer que celles-ci sont efficaces et suffisantes ;
- vérifier que la cartographie des traitements est adaptée au(x) traitement(s) effectués par l'entreprise ;
- contrôler que l'entreprise ne conserve pas de données au-delà de la période de conservation prévue et procéder à l'effacement des données concernées le cas échéant ;

Lors de chacun de ses contrôles ou réunions, le Comité de contrôle doit élaborer un compte-rendu formalisé par écrit faisant état de ses constatations et décisions prises ainsi que des délais maximums de mise en œuvre de ces dernières le cas échéant.

Chaque compte-rendu est daté, signé et conservé dans un dossier dédié auprès du Référent(e) protection des données.

## III. MESURES OPERATIONNELLES INTERNES

### A. Tenue du registre des traitements de données personnelles

Le registre de traitements a pour objet de lister et encadrer les différents traitements de données mis en œuvre par l'entreprise.

Il est mis à jour à chaque fois que nécessaire et constitue la base de notre politique interne de protection des données.

### B. Elaboration de plans de formation des collaborateurs concernés par le traitement et la protection des données personnelles

Afin de maintenir une politique efficace de protection des données, l'entreprise met en œuvre une politique de formation permettant à tout collaborateur d'appréhender la réglementation applicable en matière de protection des données et d'en maitriser les enjeux. A ce titre, tout collaborateur

pouvant être amené à collecter et traiter des données dans le cadre de ses activités doit suivre une formation adéquate au plus tard dans les deux (2) mois suivant son embauche, laquelle peut lui être délivrée soit par un organisme de formation, soit en interne par le Représentant du responsable de traitement/le Référent à la protection des données.

En plus de la formation initiale visée au premier paragraphe, le Représentant du responsable de traitement, le Référent « protection des données » et les membres du Service Réclamations des données doivent être à jour des éventuelles évolutions de la réglementation applicable et être dument formés à chaque fois que nécessaire  A ce titre, le Référent protection des données doit effectuer une veille régulière afin de se tenir au courant de l'évolution de la réglementation applicable et s'assurer ainsi, à chaque fois que cela s'avère nécessaire, que le complément de formation est octroyé aux personnels concernés afin que ceux-ci conservent un niveau de maitrise de la réglementation relative à la protection des données satisfaisant.

A ce titre, le Comité de contrôle se doit de contrôler tous les ans si les personnes visées aux termes du présent paragraphe sont suffisamment formées au regard des évolutions de la réglementation applicable, de la jurisprudence mais également des éventuels manquements constatés au cours des opérations de contrôle récurrentes ou ponctuelles.

### C. Mise en œuvre d'une charte interne d'accès et de gestion des données personnelles

Afin que seuls les collaborateurs dont les fonctions occupées au sein de l'entreprise le justifient, cette dernière met en œuvre une politique de restriction et de contrôle des accès aux données personnelles, ainsi qu'une politique de protection des données.

#### 1. Accès restreint aux données

Eu égard aux fonctions qu'elles occupent au sein de l'entreprise, les seules personnes habilitées à accéder et à traiter les données sont le personnel en vigueur, dont le registre est disponible auprès du gérant du cabinet.

Chaque personne autorisée accède aux données par le biais d'un login et d'un mot de passe ne devant être communiqués à aucun tiers, salarié ou non de l'entreprise (hormis en cas de réquisition judiciaire).

Chaque mot de passe doit être constitué au minimum d'une suite de 12 caractères et être composé à la fois de lettres, de chiffres et de symboles. Il doit être changé tous les ans.

Pour notre sécurité et le bon déroulement de notre activité, le cabinet à mis en place une procédure de Plan de continuité d'activité (PCA) et un Plan de sécurité informatique (PSSI).

Le Représentant du responsable de traitement doit pouvoir contrôler à tout moment la liste des personnes ayant accédé aux données et/ou les ayant modifiées. Pour ce faire, ils peuvent voir qui à accéder aux données via le CRM et visualiser l'historiques des modifications.

Le Représentant du responsable de traitement est le seul à pouvoir modifier la liste des personnes habilitées à accéder aux données et doit être en mesure de justifier cette liste le cas échéant, soit auprès de l'Autorité de contrôle soit auprès du Responsable de traitement lorsque l'entreprise agit en qualité de sous-traitant.

#### 2. Protection des données

Afin de protéger au maximum les droits des personnes concernées par les données personnelles qu'elle exploite, notre entreprise se doit de les protéger, tant au travers de la formation et du

comportement de ses collaborateurs par rapport à la réglementation applicable en matière de protection des données qu'au travers des mesures internes de protection qu'elle a adoptées. Cet objectif de protection repose notamment sur :

- la sécurisation de l'accès au contenant informatique des données personnelles ainsi que le contenant en lui-même par rapport à d'éventuelles tentatives de « hacking » ou de détournement des données initiées par des tiers ;
- la nécessité, en cas de perte consécutive à quelque évènement ou procédé que ce soit de tout ou partie des données, de pouvoir en récupérer une copie et/ou de pouvoir reconstituer les données perdues ou devenues inexploitables afin de pouvoir, quelle que soit la situation à laquelle notre entreprise peut être confrontée, maintenir une protection satisfaisante des données ainsi qu'un traitement conforme ;
- la protection de l'identité des personnes concernées grâce à un ou plusieurs systèmes de cryptage ou de pseudonymisation des données afin que la personne concernée par celles-ci ne puisse être directement identifiée en cas d'utilisation frauduleuse ;
- l'obligation faite à chaque personne travaillant dans l'entreprise de ne pas divulguer son mot de passe à quelque personne que ce soit et de verrouiller son poste de travail dès qu'elle s'en absente, ce quelle que soit la durée prévue de son déplacement.

Dans cette optique, notre entreprise a donc mis en œuvre les moyens de protection suivants :

- PCA = Plan de continuité d'activité
- PSSI = Plan de sécurité des systèmes d'information

### 3. Comportement à adopter par chaque collaborateur concerné par le traitement de données

Conformément à la réglementation applicable, notre entreprise, en tant que Responsable du traitement des données personnelles de ses clients qu'elle collecte et traite dans le cadre des mandats conclus avec ces derniers, mais également en sa qualité de sous-traitant des assureurs partenaires pour le compte desquels elle peut être amenée à traiter ces mêmes données en application des différentes délégations dont elle bénéficie, se doit d'ériger un niveau de protection de ces données suffisant pour éviter au maximum toute violation, détournement, utilisation frauduleuse et plus généralement toute exploitation par un collaborateur, un sous-traitant ou plus généralement un tiers n'ayant pas été préalablement autorisé par les personnes concernées ou prévue par la réglementation applicable.

Au titre de cette obligation de protection des données et donc in fine des intérêts des personnes concernées, chacun des collaborateurs de l'entreprise, préposés ou bien encore sous-traitant, se doit, en plus de l'ensemble des mesures internes décrites aux termes de la PGPD, d'adopter face au traitement de données personnelles un comportement précautionneux et responsable ne générant pas de risque supplémentaire pour les personnes concernées ou ne remettant pas en cause tout ou partie de la protection de données générées par la PGPD et l'ensemble des mesures qui la constituent.

Ainsi, chaque personne visée aux termes du présent article s'interdit notamment de :

- enregistrer, stocker, transférer ou copier, par quelque moyen que ce soit, même de manière temporaire, des données sous quelque forme que ce soit sur un support interne ou externe à l'entreprise n'offrant pas un niveau de protection équivalent à celui généré par la PGPD ;
- transférer par quelque procédé que ce soit des données à un tiers dès lors que celui-ci n'a pas préalablement justifié mettre en œuvre des mesures de protection des données offrant un niveau de sécurisation au moins équivalent à celui généré par la PGPD ;

- traiter ou autoriser un tiers à traiter des données pour une finalité pour laquelle la personne concernée n'y a pas expressément consenti au préalable.

D'un point de vue général, il est interdit à tout collaborateur de l'entreprise de traiter des données personnelles en dehors des moyens et outils mis à sa disposition par l'entreprise pour lui permettre d'effectuer les tâches qui lui incombent.

#### 4. Transfert des données à des tiers

Sauf autorisation expressément prévue aux termes d'une convention dument conclue et signée ou dument accordée, le transfert de données personnelles par notre entreprise à des tiers, que ceux-ci soient ou non situés sur le territoire de l'Union Européenne ou bien encore sur le territoire d'un état bénéficiant d'une déclaration d'adéquation est interdit.

Toute demande d'autorisation de transfert tel que visé au paragraphe précédent, pour quelque raison que ce soit et auprès de quelque personne que ce soit devra être adressée au [Référent « protection des données » afin que celui-ci puisse en amont étudier la faisabilité de l'opération de transfert et mettre en œuvre les procédures idoines.

### D. Procédure à suivre en cas de violation ou détournement des données

La violation de l'accès aux données personnelles est caractérisée dès lors qu'une personne non autorisée et/ou non sous-traitante de notre entreprise a accédé par quelque moyen que ce soit aux données traitées par cette dernière.

Le détournement des données est caractérisé dès lors qu'une personne, autorisée ou non, a traité de quelque manière que ce soit tout ou partie des données pour des finalités illégales ou différentes de celles poursuivies par notre entreprise et pour lesquelles il existe une cause légitime au traitement.

Tout détournement ou violation de données doit être déclaré à l'Autorité de contrôle dans un maximum de 72 heures à compter du moment où elle a été constatée. Cette déclaration est effectuée auprès de l'Autorité de contrôle par le Représentant du Responsable de traitement.

Dès lors qu'un détournement et/ou qu'une violation de données est constatée, celui-ci doit être sans délai porté à la connaissance du Représentant du responsable de traitement.

Dès lors qu'une violation ou qu'un détournement est constaté, le Comité de contrôle PGPD doit se réunir dans les plus brefs délais afin de voir quelles sont les failles à l'origine de la violation et/ou du détournement en vue de prendre les mesures correctives nécessaires.

Toute tentative de violation ou de détournement de données personnelles et toute violation et/ou détournement de données personnelles doivent faire l'objet d'une communication interne afin de permettre à l'ensemble des collaborateurs d'en avoir connaissance et de pouvoir ainsi adapter son niveau de vigilance et d'analyse en conséquence.

## IV. MESURES APPLIQUEES EN CAS DE SOUS-TRAITANCE

La sous-traitance est l'acte par lequel notre entreprise, en tant que responsable de traitement (ou en tant que sous-traitant si le responsable de traitement le lui a autorisé) autorise un tiers (co-courtier, mandataire d'intermédiaire, fournisseur divers, etc…) à effectuer pour son compte tout ou partie d'un traitement de données personnelles concernant ses clients et/ou collaborateurs/trices salarié(e)s.

Le principe pour qu'une sous-traitance soit conclue est que le sous-traitant mette en œuvre un ensemble de mesures, pouvant être potentiellement différentes de celles que nous avons adoptées

en interne mais présentant un niveau de protection des données et de sécurité pour les personnes concernées qui soit équivalent.

En application de ce principe, tout sous-traitant potentiel doit, avant toute opération de sous-traitance de traitement de données :

1. désigner un interlocuteur dédié compétent et apte à répondre à toute question posée par le Responsable de traitement (notre entreprise) ;
2. fournir au Représentant du responsable de traitement :
   - une cartographie des risques liés aux traitements qu'il doit mettre en œuvre pour le compte de notre entreprise ;
   - sa politique interne de gestion et de protection des données ;
   - son registre des activités de traitement.
3. signer une clause de sous-traitance conforme aux exigences de la réglementation en vigueur en vertu de laquelle il s'engage notamment à collaborer avec l'Autorité de contrôle et à accepter les audits diligentés par notre entreprise.

Chaque sous-traitance doit être préalablement à sa mise en œuvre validée par le Représentant du responsable de traitement et faire l'objet d'un contrôle régulier, au moins une fois par an, visant à vérifier le respect par le sous-traitant des obligations auxquelles il a souscrit.

Le Comité de contrôle est en charge de l'audit des sous-traitants est se doit d'effectuer ses diligences selon les mêmes principes et points de contrôles que ceux mentionnés aux termes de la PGPD. Tout audit ou contrôle doit faire l'objet d'un rapport écrit et signé par le Représentant du Responsable de traitement et l'interlocuteur désigné par le sous-traitant.

En cas de constatation d'éventuels manquements commis par le sous-traitant, le Comité de Contrôle le mentionnera dans son rapport et précisera également les mesures correctives devant être apportées par le sous-traitant en vue de se conformer soit à la législation en vigueur, soit aux exigences contractuelles du Responsable de Traitement.

Le sous-traitant devra, à compter de la réception dudit rapport, accuser réception des remarques formulées par le responsable du traitement tout en précisant les délais de mise en œuvre des mesures correctives ou bien alors en justifiant les raisons d'un éventuel refus.

## V. DUREE DE CONSERVATION DES DONNEES

La durée de conservation des données dépend de la finalité de leur collecte. Elle est détaillée dans le tableau suivant :

| **Dans quel but ?** | **Pour quelle durée maximale ?** |
|---|---|
| En cas de devis sans souscription | 3 ans |
| Pour la souscription et la gestion de votre contrat et le traitement des réclamations et contentieux | Durée du contrat et du sinistre, augmentée de la durée de la prescription |
| Pour le contrôle et le pilotage de notre activité | 5 ans |
| Pour l'amélioration continue de nos services | 6 à 12 mois |
| Pour la prospection commerciale | 3 ans |
| Pour la lutte contre le blanchiment de capitaux, le financement du terrorisme et en cas de fraude à l'assurance | 5 ans |
| Pour l'exécution de nos obligations légales | Selon les durées de conservation et de prescription applicables et notamment 10 ans à des fins comptables |
| Pour le bon fonctionnement et la sécurisation des accès à notre site internet. | 1 an |
| Pour l'utilisation des cookies | Selon les durées définies dans la politique cookies du site concerné |