# POLITIQUE GENERALE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

## HARMONIE MUTUELLE

Harmonie mutuelle

GROUPE VYV

AVANÇONS collectif

# SOMMAIRE

# 1. PREAMBULE

L'entrée en vigueur le 25 mai 2018 du règlement européen sur la protection des données (RGPD) a mis en lumière la préoccupation croissante des citoyens de l'Union sur ce sujet, en lien avec la révolution numérique en cours.

Chez Harmonie Mutuelle, nous n'avons pas attendu ce renforcement du cadre réglementaire pour nous soucier de la protection de la vie privée de nos adhérents et bénéficiaires. Au contraire, nous considérons qu'elle fait partie intégrante depuis toujours de nos engagements sociétaux en tant qu'acteur global de santé, attaché à la préservation des libertés et des droits fondamentaux de chacun.

C'est pourquoi seule la recherche de solutions utiles à nos adhérents et bénéficiaires nous guide, lors de la mise en place de nouveaux traitements de données.

**Chez Harmonie Mutuelle, nous mutualisons les risques, nous ne mutualisons pas les données personnelles.**

La présente politique de protection des données à caractère personnel témoigne de l'engagement des dirigeants et collaborateurs d'Harmonie Mutuelle, dans le cadre de leurs activités quotidiennes, pour une utilisation responsable des données personnelles.

Elle porte sur 8 domaines d'engagements forts qui sont le socle la relation de confiance qu'Harmonie Mutuelle souhaite entretenir avec ses adhérents et bénéficiaires :

1. La gouvernance interne des données à caractère personnelle
2. La collecte des données à caractère personnel
3. Les utilisations des données à caractère personnel
4. Le cadre des traitements de données de santé
5. Le cadre des traitements à visée commerciale
6. Le cadre des transferts de données à caractère personnel
7. La protection de la confidentialité
8. La mise en œuvre des droits des personnes concernées

En tant que dirigeants d'Harmonie Mutuelle, nous mettons tout en œuvre pour que ces engagements soient déclinés dans toutes les procédures et modes opératoires de l'entreprise et, afin de vérifier que nos pratiques sont en adéquation avec nos engagements, nous organisons un dispositif de contrôle interne, basé sur une surveillance continue (contrôle permanent) et un plan d'audit pluriannuel (contrôle périodique).

**Chez Harmonie Mutuelle, vos données ont la parole.**

Vous avez besoin de compléments d'informations sur la protection des données personnelles ou vous souhaitez nous faire part d'une préoccupation particulière à ce sujet ? Notre responsable Protection des Données est à votre disposition.

Par ailleurs, nous avons à cœur de maintenir un dialogue permanent avec nos adhérents et bénéficiaires sur l'évolution des usages des données à caractère personnel. Cela se traduit par des réflexions participatives menées en lien avec les instances de notre gouvernance mutualiste.

**L'appartenance d'Harmonie Mutuelle au Groupe VYV, un atout supplémentaire pour la protection de vos données.**

Depuis 2017, Harmonie Mutuelle est membre du 1er acteur global mutualiste de santé et de protection sociale, le Groupe VYV. La vocation de cette union créée par les groupes MGEN, Istya et Harmonie est de devenir un acteur référent de l'économie sociale et solidaire, en construisant l'avenir d'une protection sociale toujours plus solidaire et résistant aux seules logiques de l'offre et de la demande.

Notre affiliation au Groupe VYV ne modifie en rien les engagements que nous prenons dans cette politique. Bien au contraire, elle permettra de les renforcer via une mutualisation de moyens visant à mettre en œuvre et à vous proposer les solutions les plus pertinentes et les plus innovantes pour la gestion de vos données.

Par ailleurs nous aurons une vigilance particulière pour garantir le respect de cette politique dans le cadre de toutes les collaborations intra groupe.

# 2. NOS ENGAGEMENTS EN MATIERE DE GOUVERNANCE DES DONNEES A CARACTERE PERSONNEL

La protection des données à caractère personnel s'inscrit, chez HM, dans un cadre de gouvernance dédié, autour d'un acteur-clé : le responsable Protection des Données (autrement appelé DPO ou Data Protection Officer).

En désignant en avril 2018, un DPO interne dédié, Harmonie Mutuelle a concrétisé sa volonté d'inscrire la protection des données personnelles de façon permanente dans toutes ses activités. En effet, il nous a semblé très important que cet enjeu soit directement identifiable dans notre organisation.

Notre DPO est un spécialiste de la réglementation en matière de protection des données. Il dispose de compétences techniques spécifiques et d'une expérience reconnue.

Notre DPO jouit d'une grande indépendance vis-à-vis des directions opérationnelles de la mutuelle, et d'un soutien de ses dirigeants, de façon à pouvoir exercer sa mission sans subir d'influence préjudiciable. Ainsi ses travaux et ses avis se fondent uniquement sur le souci de ne pas nuire à la protection de la vie privée de nos adhérents et bénéficiaires.

Les missions principales confiées à notre DPO sont les suivantes :

- Vérifier la conformité des activités de traitement de données à caractère personnel vis-à-vis du RGPD
- Assister les directions de la mutuelle dans l'analyse des impacts sur la vie privée des traitements ou des projets
- Coopérer avec la CNIL et être un facilitateur dans les relations de la mutuelle vis-à-vis de l'autorité de contrôle
- Hiérarchiser les risques d'atteinte à la vie privée, afin d'orienter les priorités d'action
- Elaborer et tenir le registre des traitements de données à caractère personnel effectués sous la responsabilité de la mutuelle
- Informer et conseiller les dirigeants de la mutuelle sur tout sujet ayant trait aux données à caractère personnel

Pour assurer ses missions, le DPO travaille en étroite collaboration avec 3 autres fonctions spécialisées de l'entreprise :

- Le Chief Data Officer, a en charge l'exploitation et le développement du patrimoine informationnel de la mutuelle ;
- Le Responsable de la Sécurité du Système d'Information préconise les mesures organisationnelles et techniques permettant de protéger le système d'informations de la mutuelle contre les tentatives d'intrusion ou les violations de données ;
- Le Responsable Risques Opérationnels et Conformité a en charge la définition du dispositif de contrôle interne de la mutuelle et le plan de vérification de la conformité, au regard des risques liés à la protection des données personnelles.

Enfin, il convient de souligner qu'une ligne de reporting directe permet à notre DPO d'informer et de sensibiliser les dirigeants de la mutuelle sur l'évaluation de notre dispositif de protection des données à caractère personnel et sur les actions prioritaires à mener pour le consolider.

# 3. NOS ENGAGEMENTS CONCERNANT L'UTILISATION DES DONNEES A CARACTERE PERSONNEL

Nous nous engageons à traiter les données personnelles, uniquement dans le cadre de finalités légitimes ou légales. Cette règle impérative constitue la pierre angulaire de nos usages en matière de données à caractère personnel. En pratique, les données que nous collectons nous permettent :

**D'assurer efficacement nos missions, de la phase précontractuelle à l'exécution de nos engagements :**

Il s'agit ici d'effectuer toutes les opérations nécessaires à la passation, la gestion et l'exécution de nos engagements contractuels. Dans ce cadre, nous nous attachons particulièrement à l'identification des besoins spécifiques des demandeurs en amont de toute souscription d'un contrat d'assurance.

Ces missions comportent aussi l'élaboration de comptes techniques annuels détaillés pour les contrats collectifs santé et prévoyance. Ces comptes permettent aux employeurs et aux partenaires sociaux de piloter l'adéquation des contrats vis-à-vis des besoins des personnes couvertes. Ils ne comportent que des informations anonymes.

Par ailleurs, nous utilisons les données collectées dans pour les opérations relatives à l'organisation de la vie institutionnelle de la mutuelle (assemblée générale, conseil d'administration, instances territoriales…)

**De communiquer avec nos adhérents ou bénéficiaires et toutes les personnes intéressées par nos produits et services :**

Il s'agit, notamment, de délivrer des informations sur la vie de la mutuelle, l'évolution de nos offres, ou sur des sujets entrant dans notre mission d'acteur global de santé.

Pour certains traitements, nous sommes amenés à recueillir le consentement exprès des personnes concernées et donc à gérer la traçabilité de ce consentement.

**De remplir nos obligations légales et règlementaires et de servir nos intérêts légitimes :**

Il s'agit, notamment, de respecter nos obligations relatives à la lutte contre le blanchiment ou le financement du terrorisme, de lutter efficacement contre la fraude et de nous mettre en mesure de défendre nos intérêts en justice en conservant des éléments de preuve, le cas échéant.

Enfin il s'agit également de constituer des bases et des modèles statistiques anonymes, pour améliorer nos produits et services, ou en créer de nouveaux.

**De proposer un accompagnement et des offres utiles et adaptées :**

Il s'agit ici d'être en mesure d'identifier les besoins spécifiques de chacun afin de proposer des offres adaptées et d'assurer une relation personnalisée avec nos adhérents et bénéficiaires.

**D'offrir une meilleure expérience de navigation, personnalisée et sécurisée sur nos sites et espaces en ligne :**

Nous utilisons des cookies pour évaluer la performance de nos services en ligne, résoudre des bugs, connaître la fréquentation des pages internet…

Pour une description détaillée de ces dispositifs et de leur utilisation, nous vous invitons à solliciter notre DPO et/ou à consulter la politique spécifique.

**Combien de temps conservons-nous les données ?**

Nous ne conservons les données que le temps nécessaire à la réalisation des différentes finalités décrites ci-dessus et dans le respect des différentes dispositions légales relatives à la prescription ou à toute autre durée spécifique fixée par l'autorité de contrôle dans un référentiel sectoriel (normes pour le secteur assurance).

# 4. NOS ENGAGEMENTS SUR LES DONNEES DE SANTE

**Nous nous engageons à ne pas traiter les données à caractère personnel ayant trait à la santé de nos adhérents et bénéficiaires, pour des finalités commerciales ou pour toute finalité qui pourrait nuire à leurs intérêts.**

En tant qu'organisme d'assurance complémentaire santé, nous sommes autorisés à traiter certaines données sensibles en lien avec la santé. Ces données sont nécessaires à l'exécution du contrat d'assurance et sont limitées, en règle générale, à des informations agrégées peu significatives de l'état de santé des personnes concernées. Il s'agit, par exemple, des codes actes permettant d'effectuer les remboursements prévus par nos tableaux de garanties. Pour ces données, le consentement au traitement est lié à l'acceptation du contrat d'assurance. Dans le cadre des demandes de devis ou de prise en charge (optique, dentaire, hospitalisation), nous pouvons être amenés à recevoir des informations plus détaillées, qui ne sont alors utilisées que pour évaluer la prise en charge que nous pouvons proposer.

**En aucun cas, ces données ne sont utilisées pour moduler nos tarifs de façon individualisée pour les garanties de complémentaires santé que nous assurons.**

Lorsque la nature des garanties que nous proposons l'exige, par exemple pour la souscription de contrats couvrant l'incapacité, l'invalidité, le décès, ou encore l'assurance emprunteur, des informations à caractère médical peuvent être demandées aux personnes concernées. Ces informations sont alors traitées dans une bulle de confidentialité, placée sous la responsabilité d'un médecin. Ces dispositions visent à limiter de façon stricte l'accès à ces informations qui ne sont traitées qu'avec le consentement de l'assuré et sont destinées exclusivement au médecin conseil pour la gestion du contrat.

**Par principe, nous nous engageons à réaliser systématiquement une analyse d'impact sur la vie privée pour tout traitement comportant des données dites sensibles.** Cette analyse vise à définir les modalités de mise en œuvre du traitement, mais peut aussi nous conduire à renoncer à celui-ci.

# 5. NOS ENGAGEMENTS SUR L'USAGE COMMERCIAL DES DONNEES

Nous avons la volonté de proposer à nos adhérents et bénéficiaires des services et des offres adaptés à leurs besoins, dans le cadre d'une relation personnalisée.

Cet objectif nous amène à utiliser les données collectées et celles issues de l'utilisation de nos contrats et services, à des fins d'amélioration de nos produits. Pour cela les données sont préalablement anonymisées afin de constituer des bases statistiques.

En matière de relation, nous proposons à nos adhérents et bénéficiaires des dispositifs et des supports visant à leur apporter une information la plus pertinente possible et à fluidifier les échanges entre eux et la mutuelle. Ainsi, nous pouvons les informer sur les évolutions de nos offres et services et étudier avec eux l'adéquation de leurs contrats.

**Dans tous les cas de figures, nous engageons à respecter les choix des personnes concernées en matière de de communication et de prospection commerciale.**

# 6. NOS ENGAGEMENTS SUR LES TRANSFERTS DE DONNEES

**Nous ne communiquons aucune donnée personnelle à des tiers en dehors du cadre contractuel, sans consentement des personnes concernées.**

Les données sont uniquement destinées :

- aux personnels habilités de la Mutuelle,
- aux éventuels sous-traitants missionnés par la Mutuelle et contribuant à la réalisation des finalités mentionnées dans cette politique,
- aux partenaires et organismes professionnels dont l'intervention est prévue contractuellement,
- aux organismes officiels et aux autorités administratives ou judiciaires, pour satisfaire aux obligations légales et règlementaires.

**En aucun cas, les données personnelles que nous collectons ne font l'objet d'un transfert à titre onéreux auprès de tiers.**

**Lorsqu'un transfert de données à caractère personnel est prévu contractuellement, nous nous engageons à nous assurer qu'un niveau de sécurité adéquat est maintenu tout au long de la chaîne de traitement.**

# 7. NOS ENGAGEMENTS POUR LA PROTECTION ET LA CONFIDENTIALITE DES DONNEES

La sécurité des données est un enjeu majeur pour Harmonie Mutuelle. C'est pourquoi nous mettons en œuvre des dispositifs organisationnels et techniques pour maîtriser les risques de sécurité informatique.

Une organisation dédiée à la sécurité des systèmes d'information

La stratégie de sécurisation des systèmes d'information est pilotée par le Responsable de la Sécurité des Systèmes d'information (RSSI) et une équipe dédiée. Cette équipe s'appuie également sur :

- Une équipe de sécurité opérationnelle, dédiée à la gestion des problématiques techniques de sécurité au sein d'Harmonie Mutuelle ;
- Les directeurs des départements en charge du système d'information, responsables du respect des exigences de sécurité dans leurs équipes respectives et de relayer les bonnes pratiques de sécurité ;
- Plus globalement, l'ensemble des collaborateurs d'Harmonie Mutuelle, faisant l'objet de campagnes de sensibilisation spécifiques afin de leur donner les bons réflexes de sécurité vis-à-vis des données personnelles qu'ils pourraient être amenés à manipuler.

La Politique Générale de Sécurité SI (PGSSI), approuvée par les dirigeants de la Mutuelle, fixe les lignes directrices de la sécurité d'Harmonie Mutuelle. Cette politique, et plus généralement la démarche de sécurisation, s'appuie sur les normes ISO 27001 et 27002 reconnues internationalement. Cette démarche vise à :

- Evaluer les risques de sécurité portant sur les informations confidentielles manipulées par les collaborateurs, et particulièrement les données personnelles ;
- Assurer que des mesures de sécurité appropriées sont prises afin d'assurer la protection des informations contre ces risques.

Le RSSI et le DPO Harmonie Mutuelle coordonnent ainsi leurs actions pour s'assurer que les données personnelles confiées à Harmonie Mutuelle sont sécurisées sur l'ensemble de leur chaîne de traitement, aussi bien chez Harmonie Mutuelle que ses sous-traitants.

**Des mesures organisationnelles et techniques de sécurité adaptées pour assurer la confidentialité et l'intégrité des données personnelles**

Harmonie Mutuelle a défini un ensemble de principes de sécurité informatique autour des données personnelles :

- Limiter strictement les accès aux données personnelles aux seules personnes autorisées ;
- Détecter et corriger les modifications potentiellement non souhaitées sur les données personnelles ;
- Etre en mesure de tracer qui a réalisé une opération sur les données personnelles.

**Une gestion réactive et transparente des incidents de sécurité**

Nous mettons en œuvre des dispositifs permettant de détecter rapidement tout incident de sécurité affectant nos infrastructures informatiques. L'organisation définie nous permet ensuite de mobiliser toutes les expertises techniques nécessaires pour qualifier les incidents, prendre les mesures de protection et corriger les éventuelles failles.

Dans le cas d'un incident entraînant une violation de données personnelles et présentant des risques pour la vie privée, nous effectuons une notification auprès de la CNIL dans les 72 h. Nous nous engageons également à avertir par tout moyen à notre disposition les personnes concernées, afin qu'elles puissent prendre les mesures nécessaires.

# 8. NOS ENGAGEMENTS POUR LES DROITS DES PERSONNES CONCERNEES

La réglementation définit les droits des personnes concernées par les traitements de données à caractère personnel :

Droits d'accès : les personnes concernées peuvent obtenir des informations sur les traitements de leurs données à caractère personnel et une copie de celles-ci.

Droit de rectification : si elles estiment que leurs données sont inexactes ou incomplètes, les personnes concernées peuvent demander à ce qu'elles soient modifiées en conséquence.

Droit à l'effacement : dans la mesure de ce qui est permis par la loi, les personnes concernées peuvent exiger l'effacement de leurs données à caractère personnel.

Droit à la limitation du traitement : les personnes concernées peuvent demander la limitation du traitement de leurs données à caractère personnel. Ce droit s'exerce cependant dans le respect de l'intérêt légitime de la mutuelle.

Droit d'opposition : les personnes concernées peuvent s'opposer au traitement de leur données à caractère personnel, en raison de leur situation particulière. Elles disposent par exemple du droit de s'opposer à l'utilisation de leurs données personnelles à des fins de prospection commerciale et/ou de profilage.

Droit de retirer son consentement : lorsqu'elles ont consenti à certains traitements (par exemple pour l'envoi de newsletter ou d'actualités commerciales), les personnes concernées disposent du droit de retirer à tout moment ce consentement.

Droit à la portabilité des données : quand ce droit est applicable, les personnes concernées peuvent demander à ce que les données à caractère personnel qu'elles ont fournies leurs soient restituées, ou lorsque cela est possible techniquement, soient transférées à un tiers de leur choix.

Droit de définir des directives relatives à la gestion des données après le décès : les personnes concernées peuvent obtenir la mise en œuvre de leur volonté sur le sort de leurs données personnelles après leur décès.

Nous nous attachons à garantir l'accessibilité et l'effectivité de ces droits. Pour faciliter les démarches de nos adhérents et bénéficiaires, nous avons donc défini un point de contact unique :

Responsable Protection des données - Data Protection Officer - de la Mutuelle

Mail : dpo@harmonie-mutuelle.fr

Courrier postal : Harmonie Mutuelle - Service DPO - 29 quai François Mitterrand – 44273 Nantes Cedex 2

Enfin si les personnes concernées sont insatisfaites du traitement de leurs données personnelles par nos soins, elles ont la capacité de saisir l'autorité de contrôle compétente :

Commission Nationale de l'Informatique et des Libertés (CNIL)

Adresse postale : 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07

Site internet : www.cnil.fr