La Mutuelle Catalane
Une mutuelle plus humaine

DOCUMENT INTERNE

Version 4.0
Mai 2026 - mise à jour en cours
Validation : DPO - Direction Générale - Conseil d'Administration

GOUVERNANCE - CONFORMITÉ - SÉCURITÉ DES DONNÉES

Politique générale de protection des données personnelles

Conservation, archivage, destruction et continuité des données traitées par La Mutuelle Catalane.

RGPD | DORA | PCA / PRA | Données de santé | Conservation / destruction

ORGANISME

La Mutuelle Catalane
Société mutualiste régie par le Livre II du Code de la mutualité

IDENTIFICATION

N° SIREN : 302 476 536
20 Avenue de Grande-Bretagne, 66000 Perpignan

OBJET

Protection, conservation, archivage, purge, anonymisation et destruction des données personnelles.

ARTICULATION DOCUMENTAIRE

PSSI, politique de sous-traitance, PCA, PRA, gestion des incidents et prestataires critiques.

Document remplaçant la politique de protection des données mise à jour le 16 avril 2024.

Classification : usage interne / gouvernance

Sommaire

Cette version regroupe les thèmes proches afin de constituer une politique générale plus lisible, moins procédurale et mieux adaptée à une validation institutionnelle.

CORPS DE LA POLITIQUE

ANNEXES OPÉRATIONNELLES

> **Principe directeur.** La présente politique fixe un cadre institutionnel. Les modalités techniques et opérationnelles peuvent être précisées dans les procédures internes, les registres, le PCA/PRA, la PSSI, les contrats et les annexes associées.

CHAPITRE 1

Préambule, objet et périmètre

La protection des données personnelles constitue une exigence fondamentale pour La Mutuelle Catalane. En sa qualité d'organisme de complémentaire santé régi par le Livre II du Code de la mutualité, la Mutuelle traite quotidiennement des données relatives à ses adhérents, prospects, ayants droit, salariés, administrateurs, partenaires, professionnels de santé, entreprises adhérentes et prestataires.

Certaines données présentent une sensibilité particulière, notamment lorsqu'elles concernent la santé, les remboursements de soins, les garanties souscrites, la situation familiale, les coordonnées bancaires, les réclamations ou les échanges avec les services de la Mutuelle.

La présente politique définit le cadre général applicable à la protection, à la conservation, à l'archivage et à la destruction des données personnelles traitées par La Mutuelle Catalane. Elle constitue un document institutionnel de référence, destiné à être compris par la Direction Générale, le Conseil d'Administration, le DPO, le RSSI, les responsables de pôle, les collaborateurs autorisés et les prestataires concernés.

Elle poursuit cinq objectifs principaux : garantir le respect des droits des personnes concernées ; assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données ; préciser les responsabilités internes ; encadrer les traitements réalisés par les services et les prestataires ; organiser la conservation, l'archivage, la purge, l'anonymisation et la destruction des données.

Cette politique s'applique à l'ensemble des supports : applications métiers, outils bureautiques, messagerie, espaces collaboratifs, dossiers papier, archives, sauvegardes, fichiers temporaires, journaux techniques et supports utilisés en mode dégradé.

Elle s'articule notamment avec le RGPD, la loi Informatique et Libertés, le Code de la mutualité, Solvabilité II, DORA, la Politique de Sécurité des Systèmes d'Information, la Politique de sous-traitance, le Plan de Continuité d'Activité, le Plan de Reprise d'Activité et les procédures internes de gestion des incidents.

CHAPITRE 2

Principes fondamentaux de protection des données

La Mutuelle Catalane applique les principes fondamentaux de protection des données personnelles.

Les traitements sont mis en œuvre de manière licite, loyale et transparente. Les personnes concernées sont informées, selon des modalités adaptées, des finalités poursuivies, des bases juridiques applicables, des destinataires, des durées de conservation et des droits dont elles disposent.

Les données sont collectées pour des finalités déterminées, explicites et légitimes. Elles ne doivent pas être réutilisées d'une manière incompatible avec ces finalités.

La Mutuelle applique un principe de minimisation : seules les données strictement nécessaires à la finalité poursuivie peuvent être collectées, utilisées ou conservées. Les services internes doivent éviter toute collecte excessive, tout stockage inutile et toute duplication non maîtrisée.

Les données doivent être exactes, pertinentes et, si nécessaire, mises à jour. Lorsqu'une donnée est identifiée comme inexacte, obsolète ou incomplète, les services concernés doivent engager les corrections nécessaires.

La conservation des données est limitée dans le temps. Les données personnelles ne doivent pas être conservées indéfiniment. Elles sont conservées pendant une durée proportionnée à la finalité poursuivie, puis supprimées, archivées, anonymisées ou détruites selon les règles applicables.

La Mutuelle garantit l'intégrité et la confidentialité des données. Des mesures techniques et organisationnelles adaptées sont mises en œuvre pour protéger les données contre l'accès non autorisé, la divulgation, l'altération, la perte ou la destruction non autorisée.

Enfin, La Mutuelle doit pouvoir démontrer sa conformité. À ce titre, elle documente ses traitements, ses décisions, ses incidents, ses analyses, ses mesures de sécurité, ses durées de conservation et ses actions correctrices.

CHAPITRE 3

Bases juridiques, catégories de données et finalités

Les traitements de données personnelles mis en œuvre par La Mutuelle Catalane reposent sur la base juridique appropriée selon la finalité poursuivie. Ces bases peuvent notamment être l'exécution du contrat mutualiste, le respect d'une obligation légale ou réglementaire, l'intérêt légitime de la Mutuelle, le consentement lorsque celui-ci est requis, la protection des intérêts vitaux ou la constatation, l'exercice ou la défense de droits en justice.

La Mutuelle ne fonde pas systématiquement ses traitements sur le consentement. Dans le cadre de la gestion des contrats, des adhésions, des prestations, des flux, des obligations réglementaires et de la relation mutualiste, d'autres bases juridiques peuvent être plus appropriées.

Les catégories de données traitées comprennent notamment les données d'identification, les données de contact, les données contractuelles, les données relatives aux prestations, les données de santé, les données bancaires et financières, les données de communication, les données de réclamation, les données commerciales, les données RH, les données de gouvernance et les données techniques ou de sécurité.

Les traitements poursuivent notamment les finalités suivantes : gestion des adhésions et des contrats ; gestion des prestations et remboursements ; gestion des flux NOEMIE, AMC et tiers payant ; relation adhérent ; gestion commerciale et développement ; conformité, contrôle interne, lutte contre la fraude, gouvernance, comptabilité, fiscalité et reporting ; sécurité des systèmes d'information ; continuité d'activité ; gestion des droits des personnes ; gestion des incidents et des violations de données.

Les données de santé font l'objet d'une vigilance renforcée. Elles ne peuvent être traitées que dans la limite de ce qui est nécessaire à la gestion des droits, au remboursement des prestations, au contrôle des garanties, à la prévention de la fraude, à la gestion des réclamations ou au respect des obligations légales et réglementaires.

CHAPITRE 4

Gouvernance, responsabilités et pilotage

La protection des données est une responsabilité partagée entre la gouvernance, la Direction Générale, les fonctions de contrôle, les services opérationnels, le DPO, le RSSI et les prestataires.

Le Conseil d'Administration et les dirigeants effectifs portent l'engagement général de La Mutuelle Catalane en matière de protection des données, de sécurité, de continuité d'activité et de conformité. Ils veillent à ce que les moyens nécessaires soient alloués et peuvent être amenés à arbitrer les décisions majeures en cas d'incident significatif ou de crise.

La Direction Générale garantit la mise en œuvre opérationnelle de la présente politique. Elle valide les orientations, arbitre les priorités, mobilise les ressources nécessaires et assure le lien avec les instances de gouvernance.

Le RSSI pilote les mesures relatives à la sécurité des systèmes d'information, à la gestion des incidents techniques, au PCA/PRA et à la coordination opérationnelle des prestataires critiques en cas de crise. Il contribue à la qualification des violations de données, alimente le journal de crise et participe, avec le DPO, aux notifications réglementaires lorsque cela est nécessaire.

Le DPO, assuré par la société Fairstone, conseille La Mutuelle Catalane sur ses obligations en matière de protection des données. Il contribue à la conformité des traitements, participe à l'analyse des risques, intervient dans la gestion des violations de données, apprécie la nécessité d'une notification à la CNIL et constitue un point de contact pour les personnes concernées et l'autorité de contrôle.

Les responsables de pôle veillent à l'application de la présente politique dans leur périmètre. Chaque collaborateur doit respecter les règles de confidentialité, de sécurité et de protection des données dans l'exercice de ses missions et signaler sans délai toute anomalie, erreur, perte, accès non autorisé, divulgation accidentelle ou suspicion de violation de données.

CHAPITRE 5

Sécurité, continuité d'activité et reprise

La Mutuelle Catalane met en œuvre des mesures techniques et organisationnelles adaptées afin de protéger les données personnelles contre les risques d'accès non autorisé, de perte, d'altération, de divulgation ou de destruction.

Ces mesures comprennent notamment la gestion des habilitations, la limitation des accès aux seules personnes autorisées, la protection des postes de travail, l'utilisation d'outils de sécurité, la sauvegarde des données, la supervision des systèmes critiques, la traçabilité des opérations sensibles, la sensibilisation des collaborateurs et le recours à des prestataires spécialisés lorsque cela est nécessaire.

La présente politique est directement articulée avec le Plan de Continuité d'Activité et le Plan de Reprise d'Activité de La Mutuelle Catalane. En cas d'incident majeur affectant les systèmes d'information, les outils métiers, les données personnelles, les données de santé, les flux, les sauvegardes, les prestataires critiques ou les locaux, les procédures prévues par le PCA/PRA peuvent être activées.

L'objectif est de garantir la protection des personnes, la continuité des services essentiels, la disponibilité minimale des données nécessaires à l'activité, la préservation de l'intégrité des données, la confidentialité des informations, la traçabilité des décisions et le retour sécurisé à une situation normale.

Les objectifs de reprise et de perte maximale admissible de données sont définis dans le PCA/PRA. Ils guident les mesures de sauvegarde, de restauration, de continuité et de reprise d'activité. Les sauvegardes ne constituent pas un mode d'archivage définitif : elles ont pour finalité de permettre la restauration des données en cas d'incident.

CHAPITRE 6

Fonctionnement en mode dégradé

En cas d'indisponibilité d'un outil, d'un prestataire, d'un flux ou d'un système d'information, La Mutuelle Catalane peut être amenée à fonctionner temporairement en mode dégradé.

Ce mode dégradé peut notamment impliquer l'utilisation de fichiers de suivi temporaire, de modèles bureautiques normalisés, de formulaires de secours, de documents transmis par messagerie, de communications téléphoniques ou mobiles, d'un télétravail exceptionnel ou d'une priorisation des dossiers urgents.

Ces traitements temporaires doivent rester limités dans leur durée, leur périmètre et les données utilisées. Les fichiers temporaires contenant des données personnelles doivent être créés uniquement lorsqu'ils sont nécessaires, stockés dans un emplacement sécurisé, accessibles uniquement aux personnes habilitées, clairement identifiés comme temporaires, réintégrés dans l'outil métier dès le retour à la normale, puis supprimés ou archivés selon les règles applicables.

À l'issue du mode dégradé, une vérification doit être réalisée afin de s'assurer que les données réintégrées dans les systèmes métiers sont exactes, complètes et cohérentes. Cette vérification est essentielle pour préserver la qualité des droits, la fiabilité des prestations, la traçabilité des opérations et la conformité de la Mutuelle.

CHAPITRE 7

Gestion des incidents et violations de données

Toute suspicion de violation de données personnelles doit être signalée sans délai au RSSI et au DPO.

Une violation de données peut notamment résulter d'une cyberattaque, d'un ransomware, d'un phishing, d'une erreur d'envoi, d'une divulgation accidentelle, d'une perte de document, d'un accès non autorisé, d'une altération de données, d'une suppression accidentelle, d'une indisponibilité prolongée ou d'une défaillance d'un prestataire.

Le RSSI pilote l'analyse technique de l'incident, en lien avec les prestataires concernés. Le DPO évalue les conséquences de l'incident au regard des droits et libertés des personnes concernées. L'analyse doit permettre d'identifier la nature de l'incident, les données concernées, les personnes potentiellement impactées, le volume approximatif de données affectées, les causes probables, les mesures immédiates de confinement, les risques pour les personnes, les obligations de notification et les mesures correctrices.

Lorsque la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, La Mutuelle Catalane procède à une notification à la CNIL dans les meilleurs délais et, si possible, dans un délai de 72 heures après en avoir pris connaissance. Lorsque la violation est susceptible d'engendrer un risque élevé, les personnes concernées sont informées dans les meilleurs délais selon des modalités adaptées.

Toute violation, même non notifiée à la CNIL, doit être documentée. La documentation peut comprendre le journal de crise, le registre RGPD des incidents, le registre DORA/ICT le cas échéant, les éléments techniques transmis par les prestataires, les décisions prises, les notifications réalisées, les communications adressées, les mesures correctrices et la date de clôture de l'incident.

CHAPITRE 8

Sous-traitants, prestataires critiques et transferts

La Mutuelle Catalane peut recourir à des sous-traitants ou prestataires dans le cadre de ses activités. Ces prestataires peuvent intervenir notamment pour l'infrastructure informatique, les sauvegardes, le PRA, le système d'information métier, la télétransmission, le tiers payant, la signature électronique, la téléphonie, le site Internet, les formulaires, les outils commerciaux, la cybersécurité, le DPO externalisé, la comptabilité, les assemblées générales dématérialisées ou l'emailing.

Les prestataires sont classés selon leur criticité. Les prestataires critiques font l'objet d'une vigilance renforcée.

Les contrats ou avenants doivent prévoir, lorsque cela est applicable, des obligations de confidentialité, des mesures de sécurité adaptées, le respect du RGPD, l'encadrement de la sous-traitance ultérieure, la notification rapide des incidents, des engagements de continuité d'activité, un PCA/PRA chez le prestataire lorsque cela est pertinent, des engagements de service, des modalités de réversibilité, des droits d'audit ou de contrôle et des garanties relatives à la localisation et à la protection des données.

Aucun transfert de données personnelles en dehors de l'Espace économique européen ne peut être réalisé sans garanties appropriées conformément à la réglementation applicable. Toute situation impliquant un transfert international doit être analysée avec le DPO et, le cas échéant, faire l'objet d'un encadrement documentaire adapté.

CHAPITRE 9

Conservation, archivage et destruction des données

La Mutuelle Catalane applique un principe de limitation de la conservation. Les données personnelles sont conservées pendant la durée nécessaire à la finalité du traitement, puis supprimées, anonymisées, archivées ou détruites selon les cas.

La conservation active correspond à la période pendant laquelle les données sont utilisées quotidiennement par les services de la Mutuelle, notamment pour la gestion des contrats en cours, des prestations, des adhésions, des réclamations, de la relation adhérent, des demandes de devis actives, des dossiers RH et des traitements nécessaires à l'activité courante.

L'archivage intermédiaire concerne les données qui ne sont plus nécessaires à la gestion quotidienne, mais qui doivent être conservées pour répondre à une obligation légale, réglementaire, comptable, prudentielle, contractuelle, probatoire ou contentieuse. Les données archivées doivent être séparées, physiquement ou logiquement, des données utilisées en gestion courante. L'accès aux archives doit être limité aux personnes habilitées.

À l'expiration de la durée de conservation applicable, les données doivent faire l'objet d'un sort final : suppression définitive, purge applicative, anonymisation irréversible, destruction physique du support ou archivage définitif lorsque cela est justifié par une obligation particulière.

La destruction des données personnelles doit être réalisée de manière sécurisée, traçable et proportionnée. Elle peut prendre la forme d'une suppression dans une application, d'une purge, d'une suppression de fichiers temporaires, d'une anonymisation irréversible, d'une destruction

physique de documents papier, d'une réinitialisation sécurisée de supports, d'une demande de suppression adressée à un prestataire ou d'un écrasement selon les cycles de sauvegarde.

Aucune destruction ne doit être réalisée lorsqu'un litige, un contrôle, une réclamation, une demande d'autorité ou une obligation de conservation est en cours.

CHAPITRE 10

Droits des personnes, information et amélioration continue

Les personnes concernées disposent des droits prévus par la réglementation applicable, notamment le droit d'accès, le droit de rectification, le droit à l'effacement dans les cas prévus par les textes, le droit d'opposition, le droit à la limitation du traitement, le droit à la portabilité lorsque ce droit est applicable, le droit de définir des directives relatives au sort des données après le décès et le droit d'introduire une réclamation auprès de la CNIL.

Les demandes d'exercice de droits peuvent être adressées à La Mutuelle Catalane ou au DPO. Toute demande doit être transmise sans délai au service compétent et au DPO afin d'être traitée dans les délais réglementaires. La Mutuelle peut demander des informations complémentaires lorsque cela est nécessaire pour confirmer l'identité du demandeur ou comprendre précisément la demande.

La Mutuelle veille à fournir aux personnes concernées une information claire, accessible et adaptée, notamment par les documents contractuels, les bulletins d'adhésion, les formulaires, le site Internet, les mentions d'information, les communications spécifiques ou les réponses aux demandes individuelles.

La présente politique fait l'objet d'une revue périodique. Elle est notamment réexaminée en cas d'évolution réglementaire, d'évolution importante du système d'information, de changement de prestataire critique, d'incident significatif, de test PCA/PRA ou à la demande du DPO, du RSSI, de la Direction Générale ou d'une autorité compétente.

La Mutuelle organise des actions de sensibilisation et de formation afin de renforcer la culture de protection des données : principes du RGPD, droits des personnes, confidentialité, données de santé, mots de passe, phishing, signalement d'incident, conservation et destruction des données, procédures PCA/PRA et bons réflexes en situation de crise.

ANNEXE 1

Tableau de pilotage des responsabilités

Domaine	Responsable principal	Acteurs associés
Gouvernance générale	Direction Générale	Conseil d'Administration, dirigeants effectifs
Conformité RGPD	DPO	Direction Générale, RSSI, responsables de pôle
Sécurité SI	RSSI	HCI, prestataires techniques, Direction Générale
PCA/PRA	RSSI	DG, HCI, responsables de pôle, prestataires critiques
Incidents RGPD	DPO	RSSI, DG, responsables concernés
Incidents ICT/DORA	RSSI	DG, DPO, HCI, prestataires critiques
Conservation des données	Responsables de traitement internes	DPO, RSSI, responsables de pôle
Destruction des données	Responsables de pôle	DPO, RSSI, prestataires concernés
Droits des personnes	DPO	Services concernés, Direction
Sous-traitance	Direction / RSSI / DPO	Prestataires, fonctions métiers
Sensibilisation	DPO / RSSI	Direction, responsables de pôle

ANNEXE 2

Référentiel synthétique de conservation

Le tableau ci-dessous constitue un référentiel interne de principe. Les durées précises doivent être confirmées et tenues à jour dans le registre des traitements, avec l'appui du DPO, en fonction des obligations applicables à chaque traitement.

Catégorie de données	Conservation active	Archivage intermédiaire	Sort final
Données adhérents	Pendant la relation contractuelle	Selon obligations légales, réglementaires ou contentieuses	Suppression, anonymisation ou archivage justifié
Données de prestations santé	Pendant la gestion des prestations	Selon obligations probatoires, prudentielles ou contentieuses	Suppression sécurisée ou anonymisation
Données de santé	Strictement pendant la durée nécessaire	Archivage restreint si obligation ou contentieux	Suppression sécurisée
Données de télétransmission	Pendant le traitement des flux	Selon contraintes techniques, probatoires ou réglementaires	Purge ou archivage technique
Données commerciales prospects	Pendant la relation commerciale active	Selon durée définie dans le registre	Suppression ou anonymisation
Données de réclamation	Pendant l'instruction de la réclamation	Selon obligations probatoires ou contentieuses	Archivage puis destruction
Données comptables	Pendant l'exercice comptable	Selon obligations comptables et fiscales	Archivage légal puis destruction
Données RH salariés	Pendant la relation de travail	Selon obligations sociales, fiscales ou contentieuses	Archivage puis destruction
Données candidats	Pendant le processus de recrutement	Selon durée définie avec le DPO	Suppression
Données de connexion et sécurité	Pendant la période utile à la sécurité	Selon contraintes de sécurité et preuve	Purge technique
Sauvegardes	Selon cycle technique défini	Non applicable sauf besoin probatoire	Rotation, écrasement ou destruction sécurisée
Archives papier	Selon utilisation opérationnelle	Selon obligation applicable	Destruction sécurisée

ANNEXE 3

Procédure synthétique en cas de violation de données

1. **Détection**
   Toute personne identifiant une anomalie ou une suspicion de violation de données doit alerter immédiatement le RSSI, le DPO ou sa hiérarchie.

2. **Qualification**
   Le RSSI et le DPO déterminent si l'incident concerne des données personnelles, des données de santé, des données sensibles, des flux critiques ou des systèmes essentiels.

3. **Confinement**
   Les premières mesures de sécurité sont engagées afin de limiter l'impact de l'incident : isolement d'un poste, désactivation d'un compte, blocage d'un accès, arrêt temporaire d'un flux ou mobilisation d'un prestataire.

4. **Analyse des risques**
   Le DPO évalue le risque pour les droits et libertés des personnes concernées. Le RSSI documente l'analyse technique.

5. **Notification**
   La Direction Générale, avec l'appui du DPO et du RSSI, décide si une notification CNIL est nécessaire. Lorsque la notification est requise, elle est réalisée dans les meilleurs délais et, si possible, dans les 72 heures.

6. **Information des personnes**
   Lorsque le risque est élevé, les personnes concernées sont informées dans les meilleurs délais selon des modalités adaptées.

7. **Documentation**
   L'incident est documenté dans le registre RGPD et, le cas échéant, dans le registre DORA/ICT et le journal de crise.

8. **Clôture et retour d'expérience**
   À la fin de l'incident, un retour d'expérience est réalisé afin d'identifier les mesures correctrices et d'améliorer les procédures internes.

ANNEXE 4

Règles applicables aux fichiers temporaires en mode dégradé

En situation de crise ou de fonctionnement en mode dégradé, les collaborateurs peuvent être autorisés à utiliser des fichiers temporaires pour assurer la continuité minimale de l'activité.

1. Ne contenir que les données strictement nécessaires.
2. Être nommés clairement et identifiés comme temporaires.
3. Être stockés dans un espace sécurisé.
4. Ne pas être partagés au-delà des personnes habilitées.
5. Ne pas être copiés localement sans nécessité.
6. Être réintégrés dans l'outil métier dès que possible.
7. Être supprimés après réintégration et vérification.
8. Être signalés au responsable de pôle ou au RSSI lorsqu'ils contiennent des données sensibles.

ANNEXE 5

Clause de destruction sécurisée

La destruction des données personnelles doit être réalisée de manière sécurisée. Pour les supports numériques, elle peut prendre la forme d'une suppression définitive, d'une purge applicative, d'un écrasement sécurisé, d'une réinitialisation contrôlée ou d'une anonymisation irréversible.

Pour les supports papier, elle doit être réalisée par broyage sécurisé ou par tout autre procédé empêchant la reconstitution des informations. Lorsqu'un prestataire intervient dans la destruction, La Mutuelle Catalane doit pouvoir obtenir une confirmation ou une attestation lorsque cela est nécessaire.

Aucune destruction ne doit être réalisée lorsqu'un litige, une réclamation, un contrôle, une obligation légale ou une demande d'autorité impose la conservation des données concernées.