Politique de protection des données personnelles

Préambule

La Mutuelle des Chambres de Commerce et de l'Industrie (MCCI) fait partie de la SGAPS UGO qui a pour objectifs :

- De nouer des relations financières fortes et durables entre les organismes affiliés ;
- De renforcer leur développement respectif ;
- D'élaborer une stratégie de groupe ouverte aux organismes du secteur mutualiste, paritaire ou coopératif partageant les mêmes valeurs.

Tout en conservant leur identité et leur existence juridique propres, les organismes affiliés ont la volonté de s'inscrire dans un champ de synergies de développement et de mises en commun de moyens.

La SGAPS UGO exerce effectivement une influence dominante, au moyen d'une coordination centralisée, sur les décisions, y compris financières, de ses organismes affiliés. Elle dispose de pouvoirs de contrôle des organismes affiliés.

La MCCI dans le cadre de son activité est amenée à exploiter des informations confidentielles ainsi que des données massives, des données personnelles et des données de santé à caractère personnel sensibles qui concernent ses adhérents et clients.

La présente Politique exprime les engagements de la MCCI en matière de protection de la confidentialité et de protection des données personnelles et l'attachement aux des libertés et des droits fondamentaux des personnes physiques dans l'utilisation de celles-ci.

Elle est complétée de procédures et processus opérationnelles internes relatifs aux finalités des traitements de données à caractère personnel concernant les personnes, les destinataires des données, leurs durées de conservation, et les modalités d'exercice des droits des personnes, et portée à la connaissance des personnes par tout moyen et tout support.

Cadre de la politique de protection des données personnelles
Objectif et périmètre

La présente Politique décrit le dispositif que la MCCI applique en matière de protection des données personnelles pour garantir la mise en œuvre de traitements équitables et transparents.

Les grands principes déclinés dans ce document témoignent des engagements mis en œuvre par la MCCI, pour respecter les libertés et les droits fondamentaux des personnes physiques, dans le cadre de ses activités quotidiennes.

Cette Politique est actualisée régulièrement pour prendre en compte les évolutions législatives et réglementaires, et tout changement dans l'organisation de l'Institution. Elle est mise à la disposition de l'ensemble de ses Clients et Partenaires.

La présente Politique de Protection des Données Personnelles est complétée de procédures et processus opérationnels internes.

Exigences légales et règlementaires

La Politique de protection des données personnelles s'inscrit dans le respect des textes de référence suivants :

- Le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données dit Règlement RGPD.
- La Loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, dite Loi Informatique et Libertés.
- Le pack de conformité assurance de Juin 2021 établi par la Commission Nationale Informatique et Libertés (CNIL) et les organisations professionnelles du secteur de l'assurance.
- L'article 226-13 du Code pénal relatifs aux sanctions en cas de non-respect du secret professionnel.

Rôles et responsabilités
Principes d'organisation

Fonction	Missions
Direction Générale	• S'assurer globalement que l'ensemble des politiques, procédures, processus soit établi en cohérence avec la réglementation en vigueur • Valider et arbitrer les décisions relatives aux actions de mise en conformit • Déterminer le processus d'allocation budgétaire pour mettre en œuvre la stratégie de protection des données personnelles • Désigner le DPO en charge de s'assurer de la conformité de l'Institution au RGPD
Délégué à la Protection des Données (DPO)	• Informer et conseiller la Direction Générale ainsi que l'ensemble des collaborateurs sur tout sujet relatif à la protection des données • Assurer le déploiement et le respect de la Politique de Protection des Données Personnelles • Echanger avec la fonction Gestion des risques afin de s'assurer que le risque informatique est intégré dans la cartographie des risques opérationnels • Coopérer avec la CNIL • Être l'interlocuteur des personnes concernées par le traitement de leurs données à caractère personnel pour l'exercice de leurs droits (accessibilité, mise à jour, suppression…) • Mener les analyses d'impacts sur la vie privée de tout nouveau traitement

Système information	• Définir et mettre en place les mesures de protection techniques et organisationnelles relatives aux différents traitements des données. • Participer aux analyses d'impacts sur la vie privée de tout nouveau traitement • Réaliser des analyses de risques informatiques
Gestion des risques	• Mesurer l'appétence aux risques informatiques de l'Institution • Intégrer les risques informatiques dans la cartographie des risques opérationnels
Contrôle Interne	• Prendre en compte les incidents • Suivre la mise en œuvre des plans de remédiation
Audit interne	• Auditer le dispositif de gestion des données à caractère personnel en évaluant la gouvernance de la sécurité, l'analyse des risques et les plans d'actions, la mise en place des projets respectant la protection des données, la gestion potentielle des crises en cas de violation des données, la détection des incidents etc.
Conformité	• S'assurer de la conformité des activités et opérations de l'Institution aux normes législatives, réglementaires, déontologiques et professionnelles • Sensibiliser à la protection des données et aux risques de non-conformité au RGPD • Conseiller la Direction Générale
Responsables des traitements	• Définit les finalités et modalités des traitements comportant des données à caractère personnel.

Au sein de la MCCI, l'organisation de la protection des données personnelles se décline selon une approche par les risques.

La cartographie des risques opérationnels intègre l'analyse des risques de gestion des données à caractère personnel.

La MCCI met en place une organisation et des moyens techniques qui permettent d'assurer la maîtrise des risques inhérents.

Attributions et responsabilités en matière d'informatique et libertés
Règles de protection des données personnelles
Finalités et mise en œuvre des traitements

Les traitements des données personnelles mis en œuvre par la MCCI répondent à des finalités déterminées, explicites et légitimes qui sont notamment les suivantes :

- Gérer les contrats de frais de santé

- Effectuer les règlements des prestations
- Gérer les contentieux judiciaires liés aux contrats
- Exécuter les dispositions légales et réglementaires en matière de lutte contre le blanchiment et le financement du terrorisme
- Lutte contre la fraude à l'assurance

Chaque traitement mis en œuvre possède une base légale renseignée dans le registre des traitements conformément aux exigences réglementaires et dans l'intérêt légitime de la MCCI.

La MCCI collecte et traite les données personnelles de manière loyale et licite.

Les données collectées par la Mutuelle sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées.

Respect des droits des personne physiques
Dans le cadre de la mise en œuvre des traitements, la Mutuelle informe les personnes concernées de la finalité des traitements portant sur les données personnelles, des destinataires de ces traitements, de la durée de conservation des informations collectées ainsi que de leurs droits.

La Mutuelle met en œuvre les moyens nécessaires pour assurer aux personnes concernées l'exercice de leurs droits d'accès, d'information, de transparence, de rectification, d'effacement, de limitation, d'opposition ainsi que de portabilité de toute donnée à caractère personnel les concernant lorsqu'elles en font la demande. Les données peuvent être rectifiées, complétées, mises à jour, verrouillées ou effacées lorsqu'elles sont inexactes, incomplètes, équivoques, périmées ou lorsque leur collecte, utilisation, communication ou conservation est interdite.

Les droits susmentionnés peuvent être exercées par e-mail ou par courrier auprès du Délégué à la protection des données (DPO) de la Mutuelle à l'adresse suivante ;

DPO : dpo@mcci.fr – 26 rue fortuny 75017 PARIS

Destinataires des données
Les données personnelles peuvent être transmises à des sous-traitants uniquement pour le compte et selon les instructions de la MCCI dès lors que le contrat de gestion mentionne les obligations en matière de protection de sécurité et de confidentialité des données et précise les objectifs de sécurité à atteindre.

Les organismes, auxiliaires de justice et officiers ministériels dans le cadre de leurs missions de recouvrement des créances, de lutte contre la fraude externe ainsi que les Autorités de contrôle (CNIL, ACPR etc.) peuvent être destinataires des données personnelles.

En interne, la Direction Générale a accès aux données personnelles dans le cadre de ses prérogatives et dans la limite de leurs attributions respectives, peuvent avoir accès aux données personnelles, les collaborateurs habilités dans l'exécution de leurs missions.

Durée de conservation des données à caractère personnel
La Mutuelle s'engage à ne pas conserver les données personnelles pour une durée plus longue que celle initialement prévue à moins de pouvoir le justifier. En outre, elle considère la possibilité de

détruire les données à caractère personnel ou de procéder à l'anonymisation des données en effaçant de façon permanente tout lien entre les données personnelles et la personne physique concernée en cas de demande de cette dernière.

Sécurité et notification des incidents

La Mutuelle détermine et met en œuvre les moyens et les mesures techniques et organisationnelles nécessaires à la protection des traitements des données à caractère personnel pour éviter tout accès par un tiers non autorisé et prévenir toute perte, altération et divulgation des données.

Toute violation des données personnelles susceptible d'engendrer un risque pour les droits et les libertés des personnes physiques est considérée comme un incident majeur au sein de la Mutuelle.

MCCI en qualité de responsable de traitement, s'engage à notifier à la CNIL, tout incident de cette nature dans les 72 heures au plus tard après en avoir eu connaissance et dans les meilleurs délais à la personne concernée.

Commission Nationale Informatiques et Libertés (CNIL)	Autorité de publique indépendante désignée par un Etat membre pour effectuer des contrôles conformément à l'article 51 RGPD.
Données à caractère personnel	Information concernant toute personne physique identifiée ou identifiable directement ou indirectement par un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou un ou plusieurs éléments propres à son identité physique, physiologique, génétique, psychique, économique ou sociale.
Mesures techniques et organisationnelles	Ensemble d'actions prises en vue de protéger les données personnelles contre la destruction ou perte accidentelle, l'altération, la divulgation ou l'accès non autorisé, notamment lorsque le traitement suppose la transmission des données par réseau et contre toute forme illicite de traitement.
Politique	Intentions et dispositions générales exprimées par la Direction.
Responsable de traitement	Entité qui détermine, en tant que personne morale, seule ou avec d'autres, les finalités et les moyens du traitement des données personnelles.
Risque	Combinaison de la probabilité d'un événement et de ses conséquences.
SI	Ensemble des dispositifs matériels, logiciels, procéduraux, organisationnels, qui concourent à conserver, traiter et échanger des informations sous forme immatérielle et matérielle, notamment les documents et supports amovibles.
Sous-traitant	Prestataire ou délégataire qui traite des données personnelles pour le compte du responsable de traitement.
Traitement	Opération ou ensemble d'opérations réalisées sur les données personnelles de manière automatisée ou non, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou l'altération, la récupération, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou autre mise à disposition, alignement ou combinaison, la suppression, la restriction ou la destruction.

Violation des données personnelles	Incident de sécurité entraînant la destruction accidentelle ou illicite, la perte, l'altération, la divulgation ou l'accès non autorisé aux données personnelles transmises, conservées ou traitées d'une autre façon.

En cas de recours à la sous-traitance, la Mutuelle s'assure que ses Partenaires intègrent le processus de notification d'incident afin de maîtriser l'exposition aux risques et disposer le plus rapidement possible des informations nécessaires, pour répondre à l'obligation de notification.

Les modalités de traitement, de qualification, les éléments constitutifs d'une documentation des violations de données tels que prévus par la réglementation actuelle sont décrits dans une procédure interne dédiée.

Transfert des données personnelles

L'Institution n'autorise pas les transferts hors Union Européenne des données dans ses relations avec ses sous- traitants (délégataires de gestion inclus) à moins que :

- L'Etat destinataire des données personnelles dans lequel se situe la filiale du sous-traitant, offre un niveau de protection suffisante au moins équivalent à celui garanti au niveau de l'Union Européenne
- Le sous-traitant a adopté les Règles internes d'entreprise (ou BCR) qui constituent un code de conduite en matière de transferts de données personnelles depuis l'Union européenne vers des Etats tiers.

Termes et définitions

Pour les besoins et la compréhension du présent document, les termes et définitions suivants s'appliquent :