

Politique générale de protection des données à caractère personnel

Indépendants & Entrepreneurs



mutuelle-medicis.com

1 - OBJECTIFS ET CHAMP D'APPLICATION DE LA POLITIQUE	3
▶ Qui doit lire et appliquer la politique ?	
▶ L'application de la politique aux Tiers	
▶ Périmètre des flux	
2 - DÉFINITIONS	4
3 - STANDARDS ET EXIGENCES MINIMUMS DE MÉDICIS	6
▶ La transparence	
▶ La minimisation et l'adéquation	
▶ Le consentement	
▶ La durée de conservation	
▶ Le droit des personnes concernées et réponses aux réclamations	
▶ La sécurité des données	
▶ Le respect de la vie privée dès la conception et protection de la vie privée par défaut	
▶ Les relations avec les sous-traitants	
▶ La documentation	
▶ Le registre des traitements	
▶ Les exigences additionnelles : données à caractère personnel sensibles	
4 - GOUVERNANCE DES DONNÉES : MISSIONS ET RESPONSABILITÉS	10
▶ Missions et responsabilités du DPO	

1 - OBJECTIFS ET CHAMP D'APPLICATION DE LA POLITIQUE

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Objectifs

Médecis assure la protection des données obtenues dans le cadre de ses activités et se conforme aux lois et réglementations applicables en matière de protection de données à caractère personnel.

Dans ce contexte, Médecis se conforme au Règlement européen n° 2016/679 sur la protection des données personnelles du 27 avril 2016 qui est applicable depuis le 25 mai 2018.

L'objet principal de la présente politique est d'assurer la mise en place par Médecis de structures appropriées de gouvernance, de contrôle ainsi que de méthodes et procédures garantissant la conformité avec les lois et réglementations applicables en matière de protection des données à caractère personnel.

Champ d'application de la politique

La politique s'applique à l'ensemble des collaborateurs et à tous les services de Médecis.

Elle s'applique également aux associations ADEPIA-Médecis et au GERP-Médecis.

La politique s'applique à toutes les données personnelles recueillies, traitées, partagées par Médecis, à la fois en ligne et hors ligne notamment :

- Les sites internet opérés par Médecis ;
- Les pages officielles de Médecis sur les réseaux sociaux ;
- Les emails échangés au sein de la société ;
- Les conversations ou correspondances ;
- Les formulaires papiers.

Médecis réalise une communication adéquate de la présente politique. Conformément au droit du travail applicable, la présente politique est rendue obligatoire et exécutoire auprès de tous les collaborateurs de Médecis par l'une des conditions suivantes :

- Par respect d'une clause du contrat de travail pour les nouveaux collaborateurs ;
- Par tout autre moyen approprié pour rendre la politique contraignante sur les collaborateurs de Médecis.

Conformément au droit du travail applicable, à ses règles internes et aux contrats de travail, Médecis peut prendre des mesures disciplinaires à l'égard de ses propres collaborateurs, notamment en cas de non-respect des standards minimum de protection des données à caractère personnel établis par la présente politique.

► Qui doit lire et appliquer la politique ?

De manière générale, les collaborateurs de toutes les directions de Médecis prennent connaissance de la présente politique. Les élus du Conseil d'Administration de Médecis et des associations souscriptrices sont également informés de sa mise en vigueur.

► L'application de la politique aux Tiers

Sous réserve de dispositions législatives ou réglementaires contraires, la présente politique s'applique aux Tiers, tels que définit à l'article 2 de la présente politique, qui ont accès ou à qui sont transmises les données personnelles des adhérents/collaborateurs de Médecis.

Médecis leur communique une synthèse de la présente politique qui sera annexée aux contrats. Les documents contractuels signés avec les Tiers reprennent également les exigences de la présente politique et contiennent au minimum des dispositions sur les points suivants :

- Le périmètre de responsabilité ;
- La propriété des données ;
- Le respect des instructions et le recours à d'autres sous-traitants ;
- La procédure de réponses aux requêtes et demandes des personnes concernées ;
- Le sort des données à l'expiration du contrat ;
- L'obligation de sécurité et de confidentialité des données ;
- La possibilité pour Médecis de réaliser un audit auprès du Tiers ;
- La procédure en cas de violations des données (failles de sécurité).

► Périmètre des flux

Les traitements de données à caractère personnel mis en place par Médecis ne font pas l'objet de transfert hors Union européenne.

2 - DÉFINITIONS

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Dans le cadre de la présente politique, les termes employés auront le sens qui leur est donné par la présente section :

“Données à caractère personnel/Données Personnelles” désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée “Personne concernée”) ; est réputée être une “personne physique identifiable” une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu’un nom, un numéro d’identification, N° de carte d’identité, salaire/rémunération, dossiers de santé, informations de compte bancaire, habitudes de conduite ou de consommation, 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.

“Données à caractère personnel Sensibles” (exemples, liste non exhaustive) désigne les données à caractère personnel telles que :

- L’origine raciale ou ethnique, les opinions politiques ou les convictions religieuses ou philosophiques de la Personne concernée ;
- L’appartenance à une organisation syndicale ;
- La santé physique ou mentale ou les conditions/vie sexuelle de la Personne concernée ;
- Les données soumises à une réglementation spécifique (données financières, données médicales...) ;
- Les données génétiques et biométriques ;
- La commission présumée d’infraction par la Personne concernée ;
- Toutes poursuites engagées pour une infraction commise, présumée commise par la Personne concernée, la soumission de telles poursuites ou la décision de toute juridiction dans le cadre de telles poursuites.

“Personne concernée” désigne l’individu sur lequel porte les “données à caractère personnel” et qui peut être identifié ou distingué des autres, directement ou indirectement, notamment par référence à un numéro d’identification ou à un ou plusieurs éléments spécifiques, propres à ses caractéristiques physique, physiologique, mentale, économique, comportementale, culturelle ou sociale. Cela inclut les clients, prospects, et collègues anciens et actuels, qu’ils soient particuliers, entrepreneurs individuels ou les membres d’une société.

“Responsable de traitement” désigne une personne qui, seule, individuellement ou conjointement, décide quelles données à caractère personnel sont collectées, pourquoi et comment elles sont collectées et traitées. Dans la

plupart des cas, ce serait la personne ou la société qui “possède” les données. Être le Responsable de Traitement ne signifie pas qu’il a la propriété des données et qu’il puisse les divulguer ou les utiliser comme il l’entend.

Au sens du Règlement Européen sur la protection des données à caractère personnel, le Responsable de Traitement sera entendu au sens général comme le Dirigeant de l’entité, et par délégation de pouvoir expresse et écrite, les Responsables de Direction ou de métiers.

Dans le cadre des activités de Médicis, le Responsable de Traitement est la mutuelle Médicis.

“Sous-Traitant” désigne toute personne ou société, non employée du Responsable de Traitement, qui traite des données à caractère personnel au nom du Responsable de Traitement et selon ses instructions (par exemple des prestataires ou fournisseurs). Les Responsables de Traitement doivent assurer le maintien de la même obligation de diligence lorsqu’un Sous-Traitant traite des données à caractère personnel en leur nom.

“Tiers” désigne toute personne physique ou morale, autorité publique, agence ou tout autre organisme autre que la Personne concernée, le Responsable du Traitement, le Sous-Traitant et les personnes qui, sous l’autorité directe du Responsable du Traitement ou du Sous-Traitant, sont habilitées ou autorisées à traiter les données. Les partenaires commerciaux sont des Tiers au sens de la présente politique.

“Traitement de données à caractère personnel” désigne 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’accès, l’enregistrement, la copie, la reproduction, le transfert, la recherche, le tri, la conservation, le stockage, la séparation, le croisement, la fusion, la modification, la structuration, l’adaptation, la mise à disposition, l’utilisation, la divulgation, la diffusion, la communication, l’extraction, l’enregistrement, l’organisation, l’adaptation, la divulgation par transmission ou toute autre forme de mise à disposition, la dissimulation, le déplacement, le rapprochement, l’interconnexion, la limitation, l’effacement, la destruction ainsi que la mise en œuvre d’autres actions sur les données, que ce soit de manière automatique, semi-automatique ou autre. Cette liste n’étant pas exhaustive.

“Destinataire” désigne la personne physique ou morale, l’autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu’il s’agisse ou non d’un tiers.

“Consentement” de la Personne concernée désigne 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” désigne 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.

“Transfert de données” désigne toute communication, toute copie ou déplacement de données par l’intermédiaire d’un réseau, ou toute communication, toute copie ou déplacement de ces données d’un support à un autre, quel que soit ce support, dans la mesure où ces données ont vocation à faire l’objet d’un traitement dans le pays destinataire (exemple : Transfert à un fournisseur de services pour informatiser la collecte des données, *call center* étrangers, plateforme informatique internationale, maintenance IT internationale).

“Finalités de traitement” désigne l’objectif poursuivi par le traitement de données à caractère personnel ou l’objectif principal d’une application informatique de données personnelles. Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.

“Autorité de Contrôle” désigne l’autorité administrative dont le rôle est d’assurer le respect des réglementations et législations sur la protection des données à caractère personnel. A cette fin, elle peut exercer des missions de contrôle ou sanctionner les manquements constatés. Pour Médicis, qui est établi en France, il s’agit de la Commission nationale de l’informatique et des libertés (CNIL).

“Data Protection Officer” (DPO) ou Délégué à la Protection des données désigne la personne garante de la protection des données personnel au sein d’un organisme. A cet effet, elle conseille et informe le Responsable de traitement et les opérationnels sur la mise en place de nouveaux traitements conformément à la réglementation en vigueur. Elle est le point de contact de l’autorité de contrôle, répond aux demandes des personnes concernées et assiste le Responsable de traitement lors de la tenue d’étude d’impact sur la vie privée.

3 - STANDARDS ET EXIGENCES MINIMUMS DE MÉDICIS

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Médis respecte les standards et exigences suivants lors de la mise en place de la collecte et des traitements de données à caractère personnel :

► La transparence

Toutes les données à caractère personnel collectées sont collectées et traitées de manière licite, loyale, et transparente au regard de la personne concernée.

Quelle information fournir aux personnes concernées et afficher sur le site internet ?

Les informations suivantes sont mentionnées dans les mentions légales ou dans des conditions générales d'utilisation (CGU) de tout site internet opéré par Médis (internet, extranet, intranet) :

- L'identité et les coordonnées de Médis en tant que Responsable de traitement,
- Toutes les finalités du traitement ;
- Les coordonnées du Délégué à la Protection des Données (DPO) ;
- La base juridique du traitement et les intérêts légitimes poursuivis ;
- La durée de conservation ou les critères de détermination de cette durée ;
- Les destinataires des données à caractère personnel ;
- Les droits des personnes concernées ;
- Le fait que la fourniture des données dépend d'une exigence à caractère réglementaire ou contractuel ;
- Le fait que la fourniture des données conditionne la conclusion d'un contrat ;
- L'existence d'une obligation pour la personne concernée de fournir ses données ;
- Les conséquences de la non fourniture des données ;
- Le droit de retirer son consentement pour les traitements basés sur le consentement ;
- Le cas échéant, l'existence d'un traitement ultérieur pour une autre finalité et les informations qui s'y rattachent.

Quand informer les personnes ?

Médis fournit aux personnes concernées ces informations au plus tard au moment de la collecte des données à caractère personnel d'une façon concise, transparente, compréhensible, aisément accessible en des termes clairs et simples. Ces informations sont fournies par écrit (y compris par voie électronique) ou par voie orale.

► La minimisation et l'adéquation

Seules les données à caractère personnel strictement nécessaires, pertinentes et non excessives par rapport au but poursuivi par le traitement sont collectées par Médis.

Par ailleurs, les données à caractère personnel collectées sont exactes, complètes et, si nécessaire, mises à jour.

Lorsque le consentement est requis pour la mise en œuvre d'un traitement, Médis s'assure que son fichier est à jour des consentements exprimés. En d'autres termes, lorsqu'une personne retire son consentement (par exemple en cliquant sur un lien de désabonnement), Médis vérifie que ce retrait est réellement pris en compte dans les systèmes et que les données personnelles de cette personne ne seront plus traitées.

Médis met en place trois grandes catégories de traitement :

- Les traitements concernant les adhérents (adhérents, prospects) ;
- Les traitements relatifs au fonctionnement de la mutuelle et à l'activité commerciale "d'assureur" ;
- Les traitements relatifs aux collaborateurs de Médis (collaborateurs, élus, partenaires).

Avant toute collecte des données personnelles, Médis définit de façon claire tous les objectifs poursuivis par la collecte des données et s'assure que la finalité définie est compatible avec ses activités.

Les données à caractère personnel ne sont pas traitées pour une finalité ultérieure incompatible avec la finalité initiale pour laquelle les données ont été collectées. Par exemple, dans le cas d'un traitement en ressources humaines, les données personnelles d'un candidat qui postule au sein de Médis ne peuvent être réutilisées à des fins de prospection commerciale.

Pour pouvoir effectuer tout traitement ultérieur dont la finalité est incompatible avec la finalité initiale, Médis s'assure qu'elle a reçu le consentement de la Personne concernée pour cette nouvelle finalité. Dans le cas contraire, Médis s'assure de la licéité des Traitements.

► Le Consentement

Lorsque le traitement de données à caractère personnel repose sur le consentement de la personne concernée, Médis démontre que le consentement a bien été donné, qu'il a été enregistré et tracé dans un système informatique.

Médicis met en place une procédure interne relative à la gestion des consentements (suivi, retrait des consentements). La personne concernée doit être mise en mesure de retirer son consentement à tout moment et Médicis l'informe des moyens permettant de retirer son consentement notamment à travers les mentions d'information fournies au moment de la collecte des données. Ces moyens doivent permettre à la personne concernée de retirer son consentement aussi simplement qu'il a été donné (ex. lien de désinscription aux newsletters).

La procédure interne de gestion des consentements permet de répercuter les consentements et les retraits de consentement dans les applications utilisées et le système d'information.

► Durée de conservation

Médicis ne conserve pas les données à caractère personnel plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont collectées.

Dans ce cadre, Médicis met en œuvre une politique documentée de conservation des données à caractère personnel qui précise la durée de conservation, les conditions de conservation ainsi que le format de stockage des données.

De manière générale, la durée maximale de conservation des données doit être déterminée en fonction de la finalité de chaque traitement en prenant en compte les obligations légales et les bonnes pratiques professionnelles.

Par ailleurs, les données à caractère personnel sont détruites dès lors qu'elles ne sont plus nécessaires aux finalités pour lesquelles elles ont été obtenues ou enregistrées. Avant leur effacement, les données à caractère personnel sont stockées d'une manière permettant l'exercice du droit d'accès des personnes concernées. Elles peuvent être conservées pendant une durée résultant de relations ou obligations juridiques, de l'exécution d'un contrat ou de l'application de mesures précontractuelles demandées par la personne concernée.

Chaque année, Médicis procède à une revue des données. En dehors des cas dans lesquels il existe une obligation d'archivage, les données qui ne présentent plus d'intérêt sont supprimées sans délai. Lors des procédures de suppression automatique, Médicis s'assure que les données sont effectivement supprimées par l'établissement d'un certificat de destruction.

► Droit des personnes concernées et réponses aux réclamations

De manière générale, le Règlement européen sur la Protection des données accorde aux personnes concernées les droits :

- D'être informées lorsque les données à caractère personnel sont enregistrées pour la première fois par Médicis pour ses besoins propres ;
- De demander des informations sur les données enregistrées les concernant, y compris des informations concernant la source des données ;
- De demander les destinataires auxquels les données sont transférées ;
- De demander la finalité de l'enregistrement des données ;
- De demander l'accès aux données les concernant, y compris sous forme de liste fournie par écrit ou par voie électronique ;
- De demander la rectification des données, quand elles sont inexactes ;
- De demander la suppression de données si cela est légalement possible ;
- D'obtenir la limitation du traitement de leurs données à caractère personnel lorsque cela est légalement possible ;
- De s'opposer au traitement de leurs données à caractère personnel par Médicis ;
- De demander la portabilité de leurs données à caractère personnel ;
- D'obtenir toute autre information qui serait exigée par la loi.

Lorsqu'une demande de personne concernée fait valoir ces droits soit par voie écrite (y compris par voie électronique) soit par voie orale, Médicis répond à la personne concernée dans un délai de 30 jours. Si la demande est complexe ou si la personne concernée effectue un trop gros volume de demande, le délai est alors allongé à 60 jours.

Sous réserve de présenter un justificatif d'identité et en fonction du statut de la personne concernée se prévalant de ses droits, Médicis met en place une organisation interne spécifique afin de traiter les demandes :

- Le Département des Ressources Humaines examine la demande des collaborateurs ;
- Le Secrétariat général examine la demande des élus ;
- La Direction de la Relation Client examine la demande des adhérents ;

3 - STANDARDS ET EXIGENCES MINIMUMS DE MÉDICIS

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

- La Direction de la communication externe et du marketing examine les demandes des prospects.

Les éléments communiqués doivent être aisément compréhensibles.

Médecis rectifie, supprime ou complète les données à caractère personnel qui sont erronées, inutiles, incomplètes ou obsolètes au regard de la finalité du traitement, soit de sa propre initiative s'il dispose de l'information, soit à la demande de la personne concernée.

Les adhérents de Médecis disposent également d'un espace personnel en ligne qui leur permettent de changer certaines de leurs données à caractère personnel.

La personne concernée peut s'adresser au DPO de Médecis pour faire valoir ses droits.

► La sécurité des données

Des mesures de contrôle et procédures appropriées sont mises en œuvre par Médecis afin d'assurer la sécurité des données à caractère personnel et de prévenir tout accès ou divulgation non autorisés, en prenant en compte l'état actuel des technologies ainsi que l'éventuel préjudice pouvant résulter de la perte ou de l'accès non autorisé aux données.

Médecis prend des mesures raisonnables pour mettre en place des systèmes organisationnels efficaces et des mesures organisationnelles, physiques et techniques. Ces mesures concernent spécifiquement, la collecte, l'utilisation, le traitement, la transmission, le transfert, le stockage et la destruction des données à caractère personnel.

Médecis identifie les risques qui pèsent sur la vie privée des personnes engendrés par son traitement en menant des analyses d'impact sur la vie privée avant de déterminer les mesures de sécurité adéquates pour réduire ces risques, le niveau des mesures de sécurité nécessaires pour la protection des données dépendant de la sensibilité des données.

Les données à caractère personnel détenues par Médecis peuvent notamment contenir des mesures telles que la pseudonymisation, le cryptage des données personnelle, l'anonymisation des données en fonction des risques ou la capacité d'assurer la confidentialité.

► Respect de la vie privée dès la conception et protection de la vie privée par défaut

Avant la mise en œuvre de tout projet, Médecis prend en compte la protection des données à caractère personnel.

Les données doivent être protégées dès la conception, mais aussi tout au long du projet et tout au long du cycle de vie de la donnée (de la collecte à la destruction). Lorsque le traitement présente des risques sur la vie privée pour la personne concernée, Médecis réalise des études d'impact afin de déterminer les mesures de sécurité techniques et organisationnelles, qui permettent d'assurer cette sécurité de bout en bout.

Les données doivent être protégées par défaut, de manière que seules les données strictement nécessaires au regard de la finalité du traitement soient collectées. Il s'agit de paramétrer le service proposé de façon que, par défaut, la vie privée des personnes soient respectées au plus haut degré possible, sans toutefois empêcher le traitement d'atteindre sa finalité.

La protection par défaut s'applique à la quantité de données collectées, l'étendue du traitement, la durée de conservation et à l'accessibilité des données. Tous ces éléments doivent être limités au strict nécessaire.

► Relations avec les sous-traitants

Lorsque le traitement est effectué par un prestataire, Médecis choisit un sous-traitant fournissant des mesures de sécurité techniques et des mesures organisationnelles suffisantes pour s'assurer que le traitement sera effectué conformément à la présente politique.

Le contrat énonce que le sous-traitant ne doit agir que sur les instructions de Médecis et que les données qu'il manipule pour le compte de Médecis ne doivent pas être traitées ou utilisées à une fin autre que celle prévue par ledit contrat. Enfin, le sous-traitant n'acquiert aucun droit ou propriété sur les données et ne doit les communiquer à d'autres personnes même pour leur conservation.

Le contrat inclut des obligations en matière de confidentialité et de sécurité.

Le Contrat doit enfin interdire au sous-traitant de sous-traiter à son tour à un tiers tout traitement de données à caractère personnel demandé par Médecis, à moins que Médecis n'ait expressément donné l'autorisation de le faire.

► La documentation

Médecis respecte le principe de responsabilisation des responsables de traitements (principe d'*accountability* en anglais). A cet effet, Médecis conserve toutes les preuves du respect de la réglementation en matière de protection des données à caractère personnel.

► Le registre des traitements

Médecis tient un registre qui recense toutes ses activités de traitements et qui précise pour chacun d'eux, les informations suivantes :

Le DPO est responsable de la tenue du registre de Médecis. Avec la contribution des collaborateurs en charge du traitement et/ou les responsables de direction, il s'assure que tout nouveau traitement est inscrit au registre avec les informations décrites ci-dessus. Le DPO valide les traitements renseignés et veillera à la mise à jour du registre.

Ce registre est tenu sous forme électronique et est mis à disposition de l'Autorité de contrôle sur demande.

► Exigences additionnelles : données à caractère personnel sensibles

Médecis peut être amenée à collecter des données à caractère Sensible dans le cadre de ses traitements telles que le numéro d'inscription au Répertoire National d'Identification des Personnes Physiques ou des données d'infraction (extraits n°3 du casier judiciaire, attestation de non condamnation pénale). Ces données ne doivent être collectées et traitées que dans les cas suivants :

- Le traitement est nécessaire aux fins de répondre à une obligation légale ou réglementaire ;
- Le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;

Médecis conserve la preuve du fondement légal l'autorisant à traiter les données à caractère personnel sensibles.

L'accès à ces données personnelles sensibles est limité et elles ne peuvent être utilisées que pour les finalités pour lesquelles elles ont été collectées. En cas de transmission spontanée et volontaire, de données de santé par l'adhérent, Médecis procède immédiatement à la destruction de cette donnée.

Les mesures de sécurité adéquates sont mises en place pour empêcher la perte, la dégradation ou le vol de ces données.

4 - GOUVERNANCE DES DONNÉES : MISSIONS ET RESPONSABILITÉS

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

► Missions et Responsabilités du DPO

Afin de garantir la conformité des traitements de données à caractère personnel, Médicis a nommé un Délégué à la Protection des Données (DPO). Le responsable juridique de Médicis est désigné DPO.

La mission principale du DPO est de faire en sorte que Médicis soit en conformité constante avec le cadre légal relatif aux données personnelles (Règlement Européen sur la protection des données personnelles).

Cet objectif est atteint au travers des missions suivantes :

- S'assurer de la conformité des traitements réalisés au sein de Médicis,
- Être le point de contact de l'autorité de contrôle.

