

Règlement de traitement des données du groupe Sanitas

1. Introduction

Sanitas Assurance Maladie (ci-après «Sanitas») traite des données personnelles dans les domaines de la loi sur l'assurance-maladie (LAMal) et de la loi sur l'assurance-accidents (LAA) en tant qu'organe fédéral et en tant que personne morale privée dans le domaine de la loi sur le contrat d'assurance (LCA) au sens de la loi sur la protection des données (LPD).

En vertu de l'article 12 de la loi fédérale sur la protection des données (LPD) et des articles 5 et 6 de l'ordonnance sur la protection des données (OPD), Sanitas est tenue d'établir, entre autres, un règlement sur le traitement.

1.1. Objectif et portée

Le règlement sur le traitement assure la transparence nécessaire dans le contexte du traitement des données.

Le traitement des données par Sanitas doit également pouvoir être compris et évalué par des personnes non spécialistes du domaine.

Le présent règlement sur le traitement fixe les principes du traitement des données au sens de la LPD. Sanitas respecte notamment les principes suivants:

- Le traitement des données par Sanitas est basé sur des bases légales ou sur le consentement explicite de la personne concernée. Un consentement explicite doit être obtenu, entre autres, lorsqu'un profilage à haut risque est effectué par une personne privée ou lorsqu'un profilage est effectué par un organe fédéral.
- Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par la loi ou qui ressort des circonstances.
Le but du traitement des données personnelles et leur collecte doivent être expressément indiqués, être reconnaissables pour la personne concernée ou ressortir des circonstances.
- L'étendue du traitement est proportionnelle à la finalité et limitée à ce qui est nécessaire pour atteindre cette finalité.
- Les données personnelles sont détruites ou rendues anonymes dès qu'elles ne sont plus nécessaires au but du traitement.
- Les données sont protégées par des mesures de sécurité techniques et organisationnelles. Les données erronées sont corrigées.
- Les droits de la personne concernée sont respectés. Les personnes concernées reçoivent des informations complètes sur leurs données enregistrées et peuvent demander leur suppression ou leur rectification.

1.2. Actualité

Le maître du fichier vérifie chaque année l'actualité du règlement et des descriptions des fichiers et communique au CPD les éventuelles modifications ou confirme l'actualité.

1.3. Définitions et abréviations

Les abréviations suivantes sont utilisées dans le règlement sur le traitement des données:

- CPD Conseiller à la protection des données du Groupe Sanitas
- LPD Loi fédérale du 20 septembre 2020 sur la protection des données, RS 235.1
- PFPDT Préposé fédéral à la protection des données et à la transparence

- OPD Ordonnance sur la protection des données du 31 août 2022, RS 235.11
- LAMal Loi fédérale du 18 mars 1994 sur l'assurance-maladie, RS 832.10
- MC Médecin-conseil
- SMC Service médecin-conseil

2. Déclaration du fichier au PFPDT

Sanitas remplit l'obligation de présentation au PFPDT conformément à l'art. 84b LAMal.

3. Protection des données et sécurité des données

3.1. Protection des données

Le Conseil d'administration du groupe Sanitas assume la responsabilité globale du respect de la protection des données. Il délègue la mise en œuvre à la direction des sociétés du groupe.

Le Comité de direction est responsable de la mise en œuvre, de la communication, du contrôle et de la surveillance de la politique de protection des données prédéfinie dans l'ensemble du groupe Sanitas. Elle s'assure que Sanitas dispose d'une organisation efficace qui soutient le respect de la protection des données. Sanitas dispose d'un conseiller à la protection des données qui veille à l'application des directives en matière de protection des données et qui est doté des ressources personnelles et financières nécessaires.

Le conseiller à la protection des données du Groupe Sanitas (CPD) indique les principaux comportements à adopter en matière de protection des données et veille au respect des dispositions légales y relatives applicables aux entreprises du groupe Sanitas.

Le CPD, en collaboration avec les services internes responsables, édicte des directives appropriées pour le respect des lois et des normes. Celles-ci visent avant tout à créer une transparence optimale lors du traitement des données personnelles, afin de permettre une identification et une évaluation professionnelles des risques éventuels en matière de protection des données.

Les collaboratrices et collaborateurs sont responsables, dans leur domaine de compétence, du respect de toutes les dispositions légales relatives à la protection des données, en particulier du devoir d'information et de confidentialité. Ni les supérieures ou supérieurs ni les collaboratrices ou collaborateurs ne peuvent déléguer cette responsabilité. Chaque collaboratrice et collaborateur de Sanitas doit signer une déclaration de protection des données lors de son embauche. Les collaboratrices et collaborateurs de Sanitas sont en outre dans l'obligation, pendant et après la fin de leur contrat de travail, de garder le secret vis-à-vis de tiers sur les informations dont ils ont connaissance dans le cadre de leur activité professionnelle, en particulier sur les données médicales. Les supérieures et supérieurs hiérarchiques veillent à ce que les membres de leur équipe soient informés en permanence des dispositions légales et internes en vigueur.

Ce règlement de traitement règle en outre les critères d'accès et l'acquisition des droits d'accès ainsi que le traitement des informations obtenues à partir du recueil de données. Les personnes autorisées ont accès uniquement aux données personnelles dont elles ont besoin pour accomplir leurs tâches.

L'accès aux locaux dans lesquels sont traitées des données personnelles sensibles est protégé par des restrictions d'accès. Seuls les collaboratrices et collaborateurs de Sanitas ou les tiers qui ont un rapport de conseil avec Sanitas et qui ont signé une déclaration de protection des données et de confidentialité y ont accès. L'accès au Service médecin-conseil est soumis à des restrictions supplémentaires.

Les directives sur l'utilisation sûre du matériel et des logiciels, d'Internet et du courrier électronique sont en outre déterminantes.

3.2. Sécurité des données

Pour protéger les systèmes, les accès ne sont généralement possibles que si la personne qui accède au site peut se légitimer au moyen d'un nom d'utilisateur et d'un mot de passe. Les applications client et informatiques ayant accès à des données personnelles sensibles sont en outre dotés de restrictions supplémentaires.

3.2.1. Mesures générales

Les systèmes d'exploitation de Sanitas sont régulièrement contrôlés et protégés contre les attaques de logiciels malveillants. Les mesures suivantes sont prises pour protéger les fichiers contre la destruction non autorisée ou accidentelle, la perte accidentelle, les erreurs techniques, la falsification, le vol ou l'utilisation illicite et le traitement non autorisé:

- Sécurisation des données
- Établissement de protocoles
- Protection d'accès
- Réseaux sécurisés
- Communication externe (e-mail, Internet) de données personnelles sensibles uniquement avec un cryptage suffisant
- Limitation de l'accès au centre de données, aux réseaux et aux autres installations techniques de stockage et de traitement des données

3.2.2. Mesures particulières

Contrôle d'accès

L'accès aux bâtiments de Sanitas est sécurisé par un système de badges. Les visiteuses et visiteurs doivent s'annoncer à la réception. Les locaux et bâtiments contenant des installations techniques de transmission et de stockage de données, comme les serveurs, les routeurs, les commutateurs, etc. sont sécurisés par des systèmes de fermeture et/ou d'accès et ne sont accessibles qu'à un cercle restreint de personnes. Les salles et les bâtiments équipés de programmes permettant d'accéder aux collections de données sont sécurisés par des systèmes d'accès.

Contrôle des supports de données personnelles

Les mesures de restriction d'accès ainsi que de limitation d'accès servent également à contrôler les supports de données personnelles. Grâce à des mesures techniques, seules les personnes autorisées peuvent traiter des données sur des supports de données électroniques.

Contrôle du transport

Il convient d'empêcher les personnes non autorisées de lire, de copier (sur d'autres lecteurs ou supports de données), d'imprimer, de modifier ou de supprimer des supports de données.

Il est interdit d'envoyer des informations sensibles sous forme non chiffrée par courrier électronique (e-mail). Dans la mesure du possible, le transport nécessaire des informations sensibles est effectué par voie électronique et crypté selon une procédure reconnue.

Le transport physique des données est effectué au moyen d'un système de transport sécurisé; les données sont cryptées pour le transport à l'aide d'une méthode reconnue et la clé est transportée séparément.

Contrôle de la publication et description de l'interface

Les destinataires des données auxquels des données personnelles sont communiquées au moyen d'installations de transmission de données sont identifiés et le respect des exigences légales pour une communication (base légale, déclaration de consentement) est assuré. Les transferts de données sont consignés et l'identité des données est vérifiée avant leur transmission.

Contrôle de la mémoire

Des contrôles d'accès et d'autorisation (p. ex. nom d'utilisateur / mot de passe) ainsi que des applications informatiques empêchent les saisies, modifications ou suppressions non autorisées dans la mémoire. Lors du remplacement des supports de stockage de données (disques durs) ou du remplacement d'ordinateurs (PC et serveurs), nous veillons à ce que toutes les données soient effacées de manière irréversible.

Contrôle de l'utilisation

L'accès aux systèmes de traitement des données est en principe protégé par des mesures techniques et doit être autorisé pour chaque personne. Le système d'information accorde aux collaboratrices et collaborateurs des droits d'accès différenciés. L'accès des personnes autorisées est alors limité aux données dont elles ont effectivement besoin pour accomplir leurs tâches.

Droit d'accès et autorisations

L'accès aux données du traitement automatisé n'est possible pour les collaboratrices et collaborateurs qu'au moyen d'applications informatiques. Les autorisations nécessaires à cet effet doivent être demandées. Les collaboratrices et collaborateurs ne possèdent des droits d'utilisation que pour les applications informatiques dont ils ont besoin pour accomplir leurs tâches et, au sein des applications informatiques, uniquement pour les domaines fonctionnels correspondant à leurs tâches. Les demandes d'autorisation doivent être approuvées par les supérieur-es hiérarchiques responsables et par la ou le propriétaire de l'autorisation. Les autorisations doivent être retirées aux collaboratrices et collaborateurs lorsqu'elles ne sont plus nécessaires pour les tâches qui leur ont été confiées.

L'organisation interne définit les droits d'accès pour chaque collaboratrice et collaborateur via un concept d'accès. Plus les données traitées sont sensibles, plus les exigences en matière d'autorisation des personnes autorisées à y accéder sont élevées. Une liste des autorisations accordées est tenue à jour (fichier journal d'audit).

L'accès à distance aux systèmes de traitement des données n'est possible que pour les personnes spécialement autorisées et par le biais d'accès cryptés.

Contrôle des saisies

Les saisies et les mutations sont consignées. Dans la mesure où des données sont saisies ou mutées de manière automatisée (ce qui se produit principalement lors de l'échange électronique de données ou lors de traitements ultérieurs automatisés tels que les cycles de paiement, etc.), l'origine des données et la durée de traitement sont en principe consignées.

4. Procédures de traitement des données

4.1. Droit d'accès aux informations

Le conseiller à la protection des données de Sanitas est compétent pour accorder aux personnes assurées le droit de consulter leurs propres données. Il se procure les données, fournit les renseignements et veille le cas échéant à la rectification des données conformément au processus défini en interne.

Les demandes peuvent être envoyées par écrit à l'adresse suivante:

Sanitas Assurance Maladie

Conseiller à la protection des données

Jänergasse 3

8021 Zurich

4.2. Procédure de rectification

Une fois identifiées, les personnes saisies peuvent demander que les données les concernant qui sont disproportionnées ou qui ne sont pas nécessaires à l'exécution du contrat soient rectifiées ou détruites. Le conseiller à la protection des données de Sanitas statue sur de telles demandes.

4.3. Blocage des données

Toute personne figurant dans un fichier peut, après s'être identifiée, demander le blocage du traitement de ses données et notamment leur communication à des tiers. Le conseiller à la protection des données de Sanitas statue sur de telles demandes et décide des conséquences de leur mise en œuvre.

4.4. Anonymisation

Les tests et les projets sont réalisés avec des données anonymes. Les données statistiques sont rendues anonymes conformément aux dispositions légales. Il n'est pas possible d'identifier des personnes concrètes.

4.5. Archivage

Les données sont conservées conformément aux exigences légales et aux instructions internes de l'entreprise.

4.6. Sauvegarde et restauration

Des sauvegardes régulières sont effectuées pour toutes les données pertinentes et ainsi définies dans les contrats. Les bases de données sont régulièrement copiées dans un répertoire séparé, avec une sauvegarde de celui-ci. La récupération des données est assurée par le système de sauvegarde.

4.7. Établissement de protocoles

Les importations définies (voir point «Interfaces») et les connexions d'utilisateurs dans les systèmes qui autorisent la journalisation sont consignées dans un protocole. Pour contrôler le respect du règlement d'utilisation, Sanitas peut évaluer les protocoles sous forme anonyme. Si un abus est constaté ou s'il existe un soupçon d'abus, Sanitas peut procéder à une

évaluation complète de l'utilisation. Les données du protocole sont conservées pendant un an, conformément aux exigences d'audit.

4.8. Définition des collections de données

Les collectes de données de Sanitas dépendent des processus commerciaux. Il en résulte les collectes de données suivantes:

Données de base / données contractuelles

- Données sur les prestations
- Données financières
- Données provenant d'offres et de propositions
- Cas de recours
- Dossier de poursuites
- Données des appels téléphoniques
- Garanties de paiement
- Données des intermédiaires

4.8.1. Interfaces

Les descriptions d'interfaces externes pertinentes pour les affaires contiennent l'origine des données, la ou le destinataire, le but, le type de données et l'information sur la périodicité et le mode de transmission des données.

Les indications suivantes concernant la transmission des données (communication) sont consignées dans la description de l'interface:

- D'où proviennent les données?
- Qui reçoit les données?
- Dans quel but les données sont-elles transmises?
- Quelles données sont transmises?
- Quelle est la périodicité de la transmission des données?
- Qui a initié la transmission?
- Sous quelle forme les données sont-elles transmises?

4.8.2. Processus

Les données sont collectées, traitées et transmises par Sanitas selon des processus définis. Les différents processus sont consignés dans des descriptions de processus destinées à un usage interne.

4.8.3. Responsabilités

- Protection des données en général et demandes de consultation: conseiller à la protection des données de Sanitas
- Sécurité des données techniques: division informatique
- Destruction de données électroniques: division informatique
- Documents pour le médecin-conseil: médecin-conseil
- Contrôles d'accès: chargé de la sécurité Sanitas

5. Dispositions finales

5.1. Entrée en vigueur

Ce règlement remplace tous les règlements publiés précédemment. Ce document entre en vigueur au 1^{er} septembre 2023*.

5.2. Documents complémentaires

- Règlements de traitement
- Liste des activités de traitement
- Concepts d'accès aux collections de données

* Décision du Comité de direction