

Règlement de traitement pour les fichiers de données du Groupe Helsana

Valable dès le 10.02.2016

Sommaire

1. Dispositions générales	3
1.1. Bases légales	3
1.2. Objectif du règlement de traitement	3
1.3. Domaine de validité	3
1.4. Organe responsable	3
1.5. Obligation de garder le secret selon l'art. 33 LPG	3
2. Structure du système d'information Helsana	4
2.1. Structure du système d'information Helsana	4
2.2. Interfaces	4
3. Services concernés	5
3.1. Centres de services et services clients régionaux	5
3.2. Domaines d'activité	5
3.3. Propriétaire de l'application	5
4. Utilisateurs et accès aux données	5
4.1. Utilisateurs	5
4.2. Gestion des utilisateurs	5
4.3. Autorisation d'accès personnelle	6
4.4. Suppression de l'autorisation d'accès	6
4.5. Formation des utilisateurs	6
4.6. Manuels d'utilisateur et directives	6
5. Traitement des données / catégories de données	6
5.1. But des fichiers de données	6
5.2. Collecte de données	6
5.3. Catégories de données	6
5.4. Communication des données	7
5.5. Autres communications de données	7
5.6. Traitement des données sur mandat	7

6. Conservation et destruction des données	7
6.1. Obligation d'archivage	7
6.2. Destruction des données.....	7
7. Mesures techniques et d'organisation	8
7.1. Contrôle d'accès	8
7.2. Contrôle des supports de données personnelles	8
7.3. Authentification des utilisateurs	8
7.4. Contrôle de la communication	8
7.5. Transmission des données	8
7.6. Contrôle du stockage	8
7.7. Exigences techniques en matière de terminaux	9
7.8. Mesures de protection des données (confidentialité) dans le cadre des terminaux	9
7.9. Procès-verbaux	9
7.10. Développement	9
7.11. Assistance aux utilisateurs et obligation d'annoncer.....	9
7.12. Surveillance et responsabilité.....	10
8. Droits des personnes concernées.....	10
8.1. Droit d'accès	10
8.2. Demande de rectification ou de destruction	10
9. Dispositions finales.....	10
9.1. Annexes.....	10
9.2. Modifications du règlement	10
9.3. Entrée en vigueur	11
10. Annexes.....	12
10.1. Annexe 1	12
10.2. Annexe 2	13
10.3. Annexe 3	14
10.4. Annexe 4	15
10.5. Annexe 5	16
10.6. Annexe 6	17

1. Dispositions générales

1.1. Bases légales

Conformément aux arts 11 et 21 de l'Ordonnance relative à la loi fédérale sur la protection des données (OLPD) en relation avec l'art. 84 de la Loi fédérale sur l'assurance-maladie (LAMal) et l'art. 96 de la Loi fédérale sur l'assurance-accidents (LAA), Helsana a élaboré le règlement de traitement suivant relatif à la collecte automatisée de données personnelles particulièrement sensible ou de profils de personnalité.

1.2. Objectif du règlement de traitement

Le règlement de traitement décrit en particulier les procédures de traitement des données et de contrôle, ainsi que le fonctionnement du traitement électronique des données. Il contient des indications sur les organes responsables de la protection et de la sécurité des données, sur l'origine des données et les fins auxquelles elles sont communiquées régulièrement. Il décrit en outre la procédure pour l'octroi des autorisations d'accès aux modules des systèmes d'information électroniques.

1.3. Domaine de validité

Le présent règlement de traitement règle le traitement des données de l'organe exécutant Helsana Assurances SA. Les autres assureurs-maladie faisant partie du Groupe Helsana (cf. www.helsana.ch) ont mandaté Helsana Assurances SA pour exécuter leur activité d'assurance-maladie.

Le traitement des données dans le cadre de SwissDRG est réglé dans le «Règlement de traitement SwissDRG».

1.4. Organe responsable

Helsana Assurances SA est responsable de l'exécution de l'assurance-maladie et par conséquent propriétaire du fichier de données du système d'information Helsana.

Helsana Assurances SA est responsable de l'exécution de l'assurance-accidents et par conséquent propriétaire du fichier de données du système d'information Helsana.

Par les mesures prévues dans le présent règlement, Helsana veille au respect des directives.

Pour faciliter la lecture, on parlera ci-après uniquement d'Helsana.

1.5. Obligation de garder le secret selon l'art. 33 LPGA

Tous les collaborateurs sont soumis à l'obligation de garder le secret selon l'art. 33 LPGA.

En cas de violation de l'obligation de garder le secret, ils sont soumis spécialement aux dispositions pénales de l'art. 92 LAMal, respectivement de l'art. 97 LAA. Les collaborateurs sont avertis des sanctions.

En outre, chaque collaborateur signe, au moment de son entrée dans l'entreprise, une déclaration de confidentialité et de secret.

2. Structure du système d'information Helsana

2.1. Structure du système d'information Helsana

Les fichiers de données du système d'information Helsana (exécution de l'assurance-maladie et accidents) ont une structure modulaire et comprennent les sous-systèmes suivants contenant les données suivantes:

- sous-système données de contrat (nom, prénom, date de naissance, numéro d'assuré, adresse, etc.);
- sous-système offres d'assurance;
- sous-système carte d'assuré (notamment nom, adresse, numéro d'assuré de la personne assurée, couverture d'assurance, suspensions);
- sous-système règlement des prestations (données concernant les prestations);
- sous-système informations médicales (factures des fournisseurs de prestations et autres documents clients);
- sous-système documents archivés (informations méd.);
- sous-système CRM: correspondance avec les assurés (nom, adresse, contacts client, besoins du clients etc.);
- sous-système suivi sinistres stationnaires;
- sous-système case management (suivi global et personnalisé d'assurés individuels);
- sous-système réductions individuelles de primes cantonales
- sous-système assurance-accidents;
- sous-système service des poursuites;
- sous-système assurance collective, assurance du personnel Helsana.

2.2. Interfaces

Différentes interfaces, comme p. ex. MediData, rendent possible le contact direct avec les prestataires externes et les fournisseurs de prestations, par exemple en cas de décompte direct entre le fournisseur de prestations et Helsana.

Par ailleurs, il existe une interface par le biais de laquelle certains fournisseurs de prestations peuvent vérifier en ligne la couverture d'assurance d'un assuré.

La protection des données et la sécurité des données correspondante sont garanties au moyen de solutions d'authentification fortes et de technologies de cryptage et de transmission modernes.

3. Services concernés

3.1. Centres de services et services clients régionaux

L'exécution de l'assurance-maladie selon la LAMal et de l'assurance-accidents selon la LAA est assurée par les centres de services régionaux, les services clients et les agences. Pour accomplir leur mission, ceux-ci traitent des données personnelles, y compris des données personnelles particulièrement sensibles, dans le système d'information d'Helsana, respectivement dans les sous-systèmes spécifiés au chiffre 2.1.

3.2. Domaines d'activité

Les collaborateurs des domaines d'activité suivants ont accès aux domaines du système d'information d'Helsana et à ses sous-systèmes nécessaires pour l'accomplissement de leurs tâches dans le cadre de l'exécution de l'assurance-maladie et accidents:

- Service des prestations
- Service clients et vente
- Gestion des débiteurs
- Finance et Comptabilité
- Assistance
- Service du médecin-conseil
- Service juridique

3.3. Propriétaire de l'application

Les propriétaires l'application pour le système d'information Helsana, respectivement pour les sous-systèmes, veillent au respect des dispositions des directives et règlements relatifs au traitement des données.

Ils sont tenus de s'assurer que leurs données d'applications ne soient mises à disposition que dans le cadre défini par la loi.

4. Utilisateurs et accès aux données

4.1. Utilisateurs

Ont accès au système d'information Helsana:

- les collaborateurs d'Helsana, pour autant qu'ils en aient besoin pour accomplir leur mission d'exécution de l'assurance-maladie et accidents;
- les administrateurs de système d'Helsana;
- les prestataires de services mandatés par contrat.

4.2. Gestion des utilisateurs

Le service informatique d'Helsana se charge de la gestion des utilisateurs de manière centralisée.

Les collaborateurs internes sont inscrits via l'interface RH et les collaborateurs externes par le biais du Sourcing respectif. Les nouvelles identités et comptes ne sont saisis que s'il existe un contrat de travail ou un contrat de prestations de service valide.

4.3. Autorisation d'accès personnelle

A l'entrée dans Helsana, chaque utilisateur obtient ses autorisations d'accès aux informations selon un modèle dérivé de sa fonction. Tous les autres droits requis doivent être sollicités individuellement par le biais du portail des autorisations. Dans ce cas, chaque demande doit être confirmée par le supérieur direct ainsi que, selon le modèle d'autorisation, par le responsable du modèle.

4.4. Suppression de l'autorisation d'accès

Les utilisateurs du système d'information Helsana ont accès aux données aussi longtemps qu'ils en ont besoin pour exercer leur fonction. En cas de départ ou de changement de mission à l'intérieur d'Helsana, le droit d'accès est supprimé et les autorisations d'accès nécessaires pour le nouveau domaine d'activité sont attribuées selon le modèle.

4.5. Formation des utilisateurs

Les utilisateurs apprennent à utiliser les différentes applications et sous-systèmes dans le cadre de formations.

4.6. Manuels d'utilisateur et directives

Pour chaque sous-système, il existe une documentation correspondante.

Par ailleurs, le traitement des données est réglé dans des directives, règlements et manuels de prestations, ainsi que dans des listes. Celles-ci sont régulièrement actualisées par les unités d'organisation compétentes.

Les services spécialisés de la direction des unités d'organisation compétentes assurent au moyen de directives spécifiques un niveau constant de l'évaluation des prestations selon la LAMal et la LAA sur tout le territoire suisse.

4.7 Prestataires de services informatiques

Dans la mesure où l'exploitation du système d'information d'Helsana est confié à des prestataires de services informatiques externes, ces prestataires suivent dans leur domaine des règles analogues.

5. Traitement des données / catégories de données

5.1. But des fichiers de données

Les fichiers de données ont pour but l'exécution correcte de l'assurance-maladie et accidents dans le cadre du traitement des données autorisé par la loi (art. 84 LAMal; art. 96 LAA).

5.2. Collecte de données

Les données proviennent principalement des assurés eux-mêmes, des personnes et autorités autorisées par les assurés (fournisseurs de prestations selon la LAMal/LAA, assurances, autorités, etc.), du règlement des prestations ou du traitement par les fournisseurs de prestations ou les autorités (p. ex. réductions des primes).

Les données peuvent également avoir été obtenues dans le cadre de l'assistance administrative (art. 32 LPG).

5.3. Catégories de données

Les annexes 1 et 3 recensent les catégories de données des fichiers de données LAMal/LAA «Système d'information Helsana».

5.4. Communication des données

Les données sont transmises aux fins suivantes:

- obligation de renseigner et d'annoncer (tribunaux, administrations, autorités, etc.);
- examen et évaluation du droit aux prestations d'un assuré;
- coordination avec les prestations d'autres assurances sociales (assurance invalidité, assurance-accidents);
- recours
- prestataires de services informatiques

Les destinataires des données sont:

- assurés et tiers mandatés;
- fournisseurs de prestations (carte d'assuré, procédure en ligne);
- autorités (cantons, OFSP, offices AI, etc.);
- association des assureurs-maladie santésuisse, assurances partenaires;
- service juridique, services sociaux, médecins-conseils;
- prestataires de services dans le domaine du traitement des données (p. ex. auditeurs, recours)

5.5. Autres communications de données

Les autres cas de communication des données sont réglés de manière exhaustive dans les arts. 84a LAMal et 97 LAA.

5.6. Traitement des données sur mandat

Helsana traite des données personnelles du système d'information Helsana dans le cadre de l'exécution de l'assurance-maladie et de l'assurance-accidents obligatoires pour le compte de ses sociétés affiliées (cf. chiffre 1.3).

Helsana peut confier certaines parties de l'exploitation du système d'information d'Helsana et le traitement des données y relatif à des prestataires en Suisse et à l'étranger. Dans ce contexte, elle observe les conditions en vigueur en matière de protection des données. Si l'accès a lieu à partir d'un pays sans protection adéquate des données, cette protection est garantie par contrat et l'accès est dans la mesure du possible limité à des cas exceptionnels.

6. Conservation et destruction des données

6.1. Obligation d'archivage

Les documents soumis à l'obligation d'archivage sont conservés pendant toute la durée exigée par la loi et protégés contre les modifications et l'accès non-autorisés.

6.2. Destruction des données

Après expiration du délai de conservation légal, les données sont supprimées du système d'information Helsana.

7. Mesures techniques et d'organisation

7.1. Contrôle d'accès

L'ensemble des locaux d'Helsana dans lesquels sont traitées des données personnelles particulièrement sensibles sont sécurisés électroniquement ou manuellement contre l'accès de personnes non-autorisées. La gestion des clés et le contrôle électronique des accès sont consignés par les personnes compétentes dans un procès-verbal que le chargé de la sécurité physique peut à tout moment demander à consulter ou à examiner.

Les mesures de sécurité sont prises en fonction de la zone de protection. Les places de travail sont protégées contre l'accès de tiers non-autorisés.

Les locaux spéciaux et sensibles, tels que les locaux techniques et les centres de données sont sécurisés comme suit:

- L'accès aux supports de données électroniques dans les centres de données et serveurs décentralisés exploités par le service informatique d'Helsana est réservé aux personnes spécifiquement autorisées et protégé par des exigences de sécurité accrues.
- Les supports de données électroniques dans les serveurs et ordinateurs décentralisés qui ne sont pas exploités par le service informatique d'Helsana sont soumis à des mesures de sécurité comparables aux mesures applicables à ceux qui sont exploités par ce dernier.

7.2. Contrôle des supports de données personnelles

Grâce à des mesures de prévention informatiques, seules les personnes autorisées peuvent traiter les données sur les supports de données électroniques. Seules les personnes autorisées ont accès au système d'information Helsana

7.3. Authentification des utilisateurs

L'accès aux sous-systèmes du système d'information Helsana est protégé par un nom d'utilisateur et un mot de passe individuel à durée déterminée.

7.4. Contrôle de la communication

Les destinataires des données à qui on communique des données personnelles au moyen d'équipements pour la transmission des données sont identifiés par le biais des interfaces (p. ex. demandes de couverture en ligne par les fournisseurs de prestations en lien avec l'utilisation de la carte d'assuré).

7.5. Transmission des données

La transmission des données entre les terminaux de données et l'ordinateur hôte est protégée par le protocole de transmission.

7.6. Contrôle du stockage

Les utilisateurs reçoivent les autorisations spécifiques pour les mutations dans les champs de données dont ils ont besoin pour accomplir leurs tâches selon la loi sur l'assurance-maladie et la loi sur l'assurance-accidents.

7.7. Exigences techniques en matière de terminaux

L'accès au réseau interne d'Helsana est limité et protégé et surveillé par des mesures de contrôle spécifiques. Des mesures analogues existent pour les réseaux des prestataires de services informatiques externes.

7.8. Mesures de protection des données (confidentialité) dans le cadre des terminaux

Les terminaux de données sont placés dans des zones sécurisées. Les terminaux de données mobiles contiennent des mémoires de données protégées par un procédé de cryptage dépendant d'un mot de passe.

Les données imprimées sont conservées de manière à ce que des tiers (p. ex. personnel d'entretien) ne puissent pas les consulter et/ou les copier. Ces données sont conservées dans des récipients verrouillés ou détruites au moyen d'un destructeur de documents ou datarec en application d'une directive interne.

7.9. Procès-verbaux

En plus du contrôle des accès au système d'information Helsana par le biais de la procédure d'autorisation, ainsi que de la protection par le biais du nom d'utilisateur et mot de passe personnel, certains sous-systèmes disposent d'une journalisation du traitement automatique, de manière à pouvoir vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. La journalisation est effectuée en application de l'art. 10 OLPD. Les procès-verbaux de journalisation sont conservés pendant 13 mois et sous une forme répondant aux exigences de la révision. Ils sont accessibles aux seuls organes ou personnes chargés de vérifier l'application des dispositions de protection et de sécurité des données personnelles et ils ne sont utilisés qu'à cette fin. Les prestataires externes de services informatiques possèdent une réglementation sur la journalisation en partie similaire mais qui leur est propre.

7.10. Développement

La séparation entre développement, test et production est garantie. Les demandes de développement du système sont résumées, définies comme maintenance, petit projet ou projet, puis budgétisées et réalisées. Cette procédure est définie dans le cadre de la «Démarche de projet Helsana».

7.11. Assistance aux utilisateurs et obligation d'annoncer

Sur le plan professionnel, les utilisateurs sont assistés par les services spécialisés de la direction de leur domaine respectif.

Le support technique pour les terminaux de données et le réseau est assuré par le service informatique d'Helsana ou confié à un prestataire externe.

Les utilisateurs sont informés du niveau de sécurité du système d'information Helsana et des prescriptions relatives à l'utilisation du système. Ces dispositions sont décrites dans les manuels d'exploitation au chapitre Sécurité de l'information. Les sanctions encourues en cas de violations intentionnelles ou par négligence de la sécurité de l'information sont connues des utilisateurs.

Tous les utilisateurs sont tenus de signaler les constatations suivantes au propriétaire de l'application ou au représentant des utilisateurs:

- erreurs dans les données saisies; erreurs dans l'identité de la personne enregistrée (par exemple indications divergentes concernant une même personne dans les différents sous-systèmes);
- erreurs dans les données de base ou leurs structures;
- points faibles observés ou supposés, p. ex. déficiences du système en matière de sécurité;
- mesures de sécurité non-appliquées ou non-respectées;
- événements imprévus pouvant affecter la sécurité de l'information.

7.12. Surveillance et responsabilité

Les propriétaires d'application des sous-systèmes veillent à ce que les utilisateurs respectent les directives, le présent règlement de traitement et ses annexes et les prestataires de services informatiques leurs exigences contractuelles.

8. Droits des personnes concernées

8.1. Droit d'accès

Toute personne peut demander à Helsana si des données la concernant sont traitées. Le droit d'accès est réglé par les arts 8 et 9 LPD, ainsi que les arts. 1 et 2 OLPD. Toute demande d'accès doit être envoyée par écrit à l'adresse indiquée à l'annexe 6 accompagnée d'une copie d'un document d'identité.

La procédure est réglée par une directive interne.

8.2. Demande de rectification ou de destruction

Les demandes de rectification ou de destruction de données sont régies par l'art. 5 al. 2 et l'art. 25 LPD. Les demandes sont à adresser à l'adresse indiquée à l'annexe 6.

9. Dispositions finales

9.1. Annexes

Les annexes suivantes font partie intégrante du présent règlement:

Annexe 1:	Catégories de données personnelles traitées LAMal
Annexe 2:	Catégories des destinataires de données LAMal
Annexe 3:	Catégories de données personnelles traitées LAA
Annexe 4:	Catégories des destinataires de données LAA
Annexe 5:	Abréviations
Annexe 6:	Contact

Les représentants des utilisateurs des sous-systèmes gèrent les documentations relatives.

9.2. Modifications du règlement

Le présent règlement de traitement est régulièrement actualisé. Il peut être modifié à tout moment. Toute modification requiert la forme écrite.

9.3. Entrée en vigueur

Le présent règlement et ses annexes remplace le règlement du 14 octobre 2014 et entre en vigueur avec effet immédiat.

Helsana



Daniel H. Schmutz
CEO



Martin Rytz
Responsable Droit & Compliance

Distribution:

- Intranet: Standards et directives d'entreprise (SDE).
- www.helsana.ch

10. Annexes

10.1. Annexe 1

Catégories de données du fichier de données LAMal annoncé au PFPDT.

Catégories de données personnelles traitées (art. 3. al. 1, let. e OLPD):

Allemand	Français	Italien
* Name, Vorname	Nom / Prénom	Nome / Cognome
* Geschlecht	Sexe	Sesso
* Geburtsdatum / Alter	Date de naissance / âge	Data di nascita / eta
* AHV-Nummer	Numéro AVS	Numero AVS
* Sprachen	Langues	Lingue
* Nationalität / Heimatort	Nationalité / lieu d'origine	Nazionalita / luogo di appartenenza
Kantons- / Gemeindezugehörigkeit	Appartenance cantonale / communale	Attinenza cantonale / comunale
* Versichertennummer	Numéro d'assuré	Numero d'assicurato
* Adresse	Adresse	Indirizzo
Bank- / Post-Verbindungen	Coordonnées bancaires / postales	Relazione bancaria / posta
Art der Versicherung und Deckung	Genre d'assurance et de couverture	Genere d'assicurazione e coperta
Art und Umfang der Leistungen	Genre et volume des prestations	Genere e entità delle prestazioni
* Gesundheitsdaten	Données sur la santé	Dati concernenti la salute
Leistungserbringer	Fournisseur de prestations	Fornitore di prestazioni
Eintritts- / Austrittsdatum	Date d'entrée / de sortie	Data entrata / uscita
Sistierung	Suspension	Sospensione
Leistungsaufschub	Suspension des prestations	Sospensione delle prestazioni
Prämie	Prime	Premia
Prämienfakturierung	Facturation des primes	Fatturazione dei premi
Franchisen	Franchise	Franchigia
Kostenbeteiligungen	Participation aux coûts	Partecipazione ai costi
Subventionen	Subventions	Sussidi
Prämienermässigungen	Réduction des primes	Riduzione di premia
Prämienvverbilligungen Kanton	Réduction des primes par les cantons	Riduzione dei premi da parte dei cantoni
Mahndaten	Données de rappel	Dati di richiamo

* Catégorie principale

10.2. Annexe 2

Catégories de données du fichier de données LAMal annoncé au PFPDT.

Catégories de destinataires des données (art. 3, al. 1, let. f OLPD):

Allemand	Français	Italien
Versicherte	Assurés	Assicurati
Leistungserbringer	Fournisseurs de prestations	Fornitori di prestazioni
Behörden	Autorités	Autorita
Kanton	Canton	Cantone
Versicherungsgesellschaften, u.a. andere Sozialversicherer, Santésuisse, Die Schweizer Krankenversicherer	Compagnies d'assurances, par ex. autres assureurs sociaux, Santésuisse, Les assureurs suisses	Società d'assicurazione per esempio altro assicuratore so- ciale, Santésuisse, gli assicura- tore svizzero
Service juridique	Service juridique	Servizio giuridico
Sozialdienste	Service social	Servizio sociale
Vertrauensärzte	Médecins-conseils	Medico di fiducia

10.3. Annexe 3

Catégories de données du fichier de données LAA annoncé au PFPDT.

Catégories de données personnelles traitées (art. 3. al. 1, let. e OLPD):

Allemand	Français	Italien
* Name, Vorname	Nom / Prénom	Nome / Cognome
* Geschlecht	Sexe	Sesso
* Geburtsdatum / Alter	Date de naissance / âge	Data di nascita / eta
* Versichertennummer	Numéro d'assuré	Numero d'assicurato
* Adresse	Adresse	Indirizzo
Bank- / Post-Verbindungen	Adresse bancaire / postale	Relazione bancaria / posta
Art der Versicherung und Deckung	Genre d'assurance et de couverture	Genere d'assicurazione e coperta
Art und Umfang der Leistungen	Genre et volume des prestations	Genere e entita delle prestazioni
* Gesundheitsdaten	* Données sur la santé	Dati concernenti la salute
Eintritts- / Austrittsdatum	Date d'entrée / de sortie	Data entrata / uscita
Leistungsaufschub	Suspension des prestations	Sospensione delle prestazioni
Prämie	Prime	Premia
Zahlungen	Paiements	Pagamenti
Zustelladresse	Adresse de livraison	Indirizzo di consegna
Begünstigtenadresse	Adresse bénéficiaire	Indirizzo beneficiando
Debitoren / Kreditoren	Débiteurs / créanciers	Debitori / creditori
Lohnsummen	Sommes salariales	Libro paga
Berufsbranche / Funktion im Unternehmen	Industrie d'emploi / fonction dans l'entreprise	Industria Job / funzione aziendale
Leistungsabzüge / Kürzungen	Déductions de prestations / réductions	Deduzioni prestazioni / riduzioni
Mahndaten	Données de rappel	Dati di richiamo

* Catégorie principale

10.4. Annexe 4

Catégories de données du fichier de données LAA annoncé au PFPDT.

Catégories de destinataires des données (art. 3, al. 1, let. f OLPD):

Allemand	Français	Italien
Versicherte	Assurés	Assicurati
Leistungserbringer	Fournisseurs de prestations	Fornitori di prestazioni
Behörden	Autorités	Autorita
Versicherungsgesellschaften	Compagnies d'assurances	Società d'assicurazione
Leistungsempfänger	Bénéficiaire de prestation	Beneficiario della prestazione
Begünstigte	Bénéficiaire	Beneficiario

10.5. Annexe 5

Abréviations

LPGA	Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (RS 830.1)
LPD	Loi fédérale du 19 juin 1992 sur la protection des données (RS 235.1)
RH	Ressources humaines
LAMal	Loi fédérale du 18 mars 1994 sur l'assurance-maladie (RS 832.10)
LAA	Loi fédérale du 20 mars 1981 sur l'assurance-accidents (RS 832.20)
SMC	Service du médecin-conseil
OLPD	Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (RS 235.11)

10.6. Annexe 6

Adresse de contact:

Les demandes de renseignements, de rectification ou de destruction doivent être adressées à:

Helsana Assurances SA
Chargé de la protection des données
Case postale
8081 Zurich