Déclaration de protection des données et règlement de traitement des données concernant les assurances-accidents d'Helsana

Version 2.0 du 03.09.2019

1. Bref aperçu

Les employés sont obligatoirement assurés par leur employeur contre les accidents conformément à la loi fédérale sur l'assurance-accidents (**LAA**). Les indépendants peuvent s'assurer volontairement contre les accidents selon la LAA. Des prestations sont versées par l'assurance-accidents obligatoire en cas d'accident professionnel et pour les maladies professionnelles et, pour les travailleurs dont le temps de travail hebdomadaire chez le même employeur est d'au moins huit heures, pour les accidents non professionnels. Les prestations couvertes sont les frais de traitement, les indemnités journalières, les rentes, les indemnités pour atteinte à l'intégrité et les allocations pour impotent.

Les prestations provisoires et durables de l'assurance-accidents obligatoire peuvent être complétées au moyen d'une assurance-accidents complémentaire. Il est par exemple possible d'assurer des salaires plus élevés que le montant maximum obligatoire du salaire assuré ou d'améliorer le confort hospitalier en passant de la division commune à la division demi-privée ou privée.

Comme d'autres assureurs-accidents privés, caisses d'assurance-accidents publiques et la SUVA, Helsana Accidents SA peut participer à l'exécution de l'assurance-accidents obligatoires selon la LAA. Helsana Accidents SA propose en outre une assurance-accidents complémentaire conformément à la loi fédérale sur le contrat d'assurance (**LCA**). Les assurances-accidents selon la LAA et la LCA peuvent être complétées par une assurance de capital de Solida Assurances SA (appelées toutes deux ensemble **Helsana**) en cas de décès et d'invalidité suite à un accident.

En cas d'exécution de l'assurance-accidents, en particulier pour le calcul des primes, de l'évaluation des prestations ou de recours envers des tiers responsables, Helsana traite les données personnelles. Par données personnelles, il faut entendre toutes les indications et informations qui se rapportent à une personne (physique) identifiée ou identifiable. Il s'agit d'une part de données de clients privés assurés chez Helsana et qui communiquent eux-mêmes leurs données à Helsana. Mais Helsana traite d'autre part aussi les données d'employés de clients Entreprises qui transmettent eux-mêmes ou par le biais de leur employeur des données dans le cadre d'une déclaration d'accident et de la gestion des accidents. Ces données personnelles incluent par exemple les coordonnées telles que le nom, l'adresse ou le numéro de téléphone. Pour accomplir son mandat légal ou contractuel, Helsana a besoin de données personnelles supplémentaires, par exemple la date de naissance, le numéro AVS et d'assuré ainsi que des informations sur la santé des personnes.

Comme Helsana accorde une grande importance à la protection de ces données parfois sensibles, la présente déclaration de protection des données indique :

- qui est responsable du traitement des données ;
- quelles personnes collectent et traitent quelles données ;
- comment et par qui les données sont collectées et traitées ;
- à quelle fin les données sont traitées et sur quelle base légale ;
- à qui les données sont divulguées ;
- combien de temps les données sont conservées ;
- quels sont les droits des personnes concernées.

2. Applicabilité de la déclaration de protection des données

La présente déclaration de protection des données explique l'obtention et les traitements ultérieurs des données personnelles par Helsana en relation avec les assurances-accidents. Elle sert parallèlement de règlement de traitement des données au sens des art. 11 et 21 de l'ordonnance relative à la loi fédérale sur la protection des données **(OLPD)** en liaison avec les art. 96 à 98 LAA.

L'obtention et le traitement ultérieur de données personnelles qui sont couvertes par d'autres déclarations de protection des données ou conditions d'utilisation, qui résultent des circonstances ou qui sont réglées par la loi demeurent réservés.

3. Responsables, délégué à la protection des données

Helsana est l'instance responsable pour l'obtention et le traitement supplémentaire des données personnelles en relation avec la mise en œuvre de l'assurance-accidents (notamment au sens de l'art. 4, al. 7 du règlement général de l'UE sur la protection des données et de la loi fédérale sur la protection des données, pour autant que les dispositions respectives soient applicables dans le cas particulier).

Les éventuelles demandes, prétentions ou demandes de renseignements en lien avec la protection des données qui concernent Helsana peuvent être adressées avec la copie d'une pièce d'identité officielle au délégué à la protection des données d'Helsana, à l'adresse suivante :

Helsana Accidents SA
Délégué à la protection des données
Case postale
8081 Zurich

4. Collecte, traitement et utilisation des données personnelles

4.1 Personnes concernées

Helsana collecte et traite les données personnelles de

- personnes – pour les salariés via leur employeur – qui sont ou étaient assurées chez Helsana ou auprès d'un autre assureur-maladie du Groupe Helsana ;
- personnes dont l'employeur est affilié à Helsana par la caisse supplétive afin de veiller au respect de l'obligation de s'assurer (cf. art. 73 al. 2 LAA) ;
- participants à des concours, à des études de marché, à des enquêtes de satisfaction et à des sondages d'opinion effectués par Helsana ;
- personnes éventuellement ou effectivement intéressées par les produits et prestations d'Helsana ;

(qualifiées toutes ensemble de **clients**).

Helsana collecte et traite par ailleurs des données de fournisseurs de prestations, de médecins-conseils, de prestataires, de partenaires de vente et d'autres partenaires commerciaux d'Helsana ainsi que de leurs collaborateurs et contacts **(partenaires)**.

Helsana traite notamment les catégories suivantes de données personnelles de clients :

- **données personnelles et coordonnées :** celles-ci incluent notamment mais non exhaustivement le prénom et le nom, le sexe, la date de naissance, l'âge, l'état civil, le numéro AVS et d'assuré, les langues, la nationalité, l'appartenance à un canton et à une commune, l'adresse (électronique), le numéro de téléphone, les données de santé (p. ex déclaration de santé), les membres de la famille, etc. ;
- **données en relation avec la communication :** celles-ci incluent des informations, telles que le canal de communication privilégié, la correspondance et la communication avec Helsana par courrier, courriel, téléphone, ou les autres modalités (y compris les enregistrements de la communication), la satisfaction des clients, etc. ;
- **données du contrat :** type d'assurance et couverture, nature et étendue des prestations, date d'entrée et de sortie, suspension ;
- **données en relation avec les règlements de prestations :** celles-ci incluent notamment les fournisseurs de prestations, les diagnostics, les rapports médicaux, les données fournies par les médecins-conseils, les coûts des prestations, les coordonnées bancaires et postales, les paiements, les données d'assureurs tiers, les informations en relation avec les demandes de renseignements, les factures du fournisseur de prestations ;
- **données en relation avec le calcul et la collecte des primes :** elles incluent notamment la prime d'assurance, la facturation des primes, les données d'encaissement, les informations sur la solvabilité, etc. ;
- **données en relation avec les litiges :** celles-ci incluent notamment les données concernant les recours et les différends en matière de prestations et de contrats afférents, par exemple les recours et les litiges ainsi que les données des dossiers de procédure des autorités et des tribunaux, etc. ;

- **données en relation avec le marketing de produits et de prestations :** celles-ci incluent des informations telles que les documents reçus et les activités spéciales, les newsletters, les préférences personnelles et les centres d'intérêt, etc. ;
- **données en relation avec le case management :** informations sur la santé, l'employeur et les conditions de travail, la situation médicale, sociale et spécifique au poste de travail et le besoin de soutien correspondant, etc.

(qualifiées toutes ensemble de **données du client**).

Par ailleurs, Helsana traite notamment les catégories suivantes de données personnelles de partenaires :

- **données des fournisseurs de prestations, des prestataires et des autres partenaires commerciaux et informations sur leurs collaborateurs et contacts**, notamment coordonnées, informations sur la fonction, informations sur les relations précédentes avec ces personnes, informations sur les activités de marketing (p. ex. réception de newsletters), informations sur les transactions commerciales, demandes, offres, propositions, conditions et contrats (notamment en relation avec les conventions tarifaires), informations sur les formations et l'activité professionnelle, etc. (**données de partenaire**).

Dans le cadre de leur relation commerciale, les clients devront mettre à disposition les données clients nécessaires ou prescrites par la loi pour engager et mettre en œuvre la relation contractuelle et exécuter les obligations contractuelles afférentes nécessaires ou prescrites par la loi. Sans ces données, Helsana ne sera généralement pas en mesure de conclure ou d'exécuter le contrat avec le client correspondant. Par analogie, cela vaut également pour les données de partenaires, pour autant qu'il s'agisse de relations d'affaires avec des prestataires, des fournisseurs et des partenaires commerciaux d'Helsana ; celles-ci ne peuvent en principe pas être conclues ni mises en œuvre sans informations sur leurs collaborateurs et les autres contacts.

4.2 Sources des données

Les données personnelles sont avant tout collectées lors de la communication directe avec les clients (courrier, formulaires de contact et de proposition, courriel, téléphone, utilisation du site Internet ou de toute autre manière).

Les données personnelles peuvent également être collectées indirectement, notamment par

- des personnes et instances mandatées par les clients (en particulier l'employeur);
- d'autres assureurs au sens de l'art. 68 al. 1 LAA en dehors du Groupe Helsana (p. ex. compagnies d'assurance privées, caisses d'assurance-accidents publiques et caisses-maladie), les caisses supplétives ou la SUVA (art. 97 LAA) ;
- des médecins-conseils :
- échange d'informations dans le cadre de l'assistance administrative (art. 32 de la loi fédérale sur la partie générale du droit des assurances sociales [**LPGA**]) et art. 98 LAA);
- des sources publiquement accessibles (p. ex. Internet, presse, médias, registre) ;

et dans le domaine des clients Entreprises par

- l'achat d'informations complémentaires provenant de sources de données de tiers (p. ex. revendeurs d'adresses).

4.3 Personnes qui traitent les données et services impliqués

La mise en œuvre de l'assurance-accidents est en premier lieu assurée par des collaborateurs des services Clients régionaux et des agences générales / points de vente Helsana. Pour cette tâche, ils traitent des données personnelles, y compris des données personnelles sensibles du fichier d'Helsana (cf. ch. 9).

Lors de la mise en œuvre de l'assurance-accidents obligatoire, les collaborateurs ont accès aux données requises pour l'exécution des tâches correspondantes, dans le cadre des activités de traitement des données (les **activités de données**) énoncées ci-après :

- gestion des canaux de vente et soutien à la vente ;
- élaboration des offres ;
- affaires avec de nouveaux clients ;
- service Clients ;
- gestion des contrats ;
- gestion des prestations ;
- achat de prestations ;
- assurance du personnel ;
- des médecins-conseils :
- sciences de la santé ;
- encaissement, finances, actuariat ;
- audit, Risk, Legal et Compliance ;
- gestion informatique et gestion de la sécurité des données ;
- fondation de prévoyance du personnel (notamment en cas de surindemnisation) ;
- achat.

Des responsables de processus veillent au respect des dispositions des directives et règlements sur le traitement des données en relation avec les activités de données chez Helsana. Il est de leur responsabilité que leurs données d'application ne soient mises à disposition que dans le cadre défini par la loi.

4.4 Décisions individuelles automatisées

Des décisions individuelles automatisées sont prises chez Helsana dans le cadre du règlement de prestations. Lorsque des clients ou des fournisseurs de prestations remettent une facture à Helsana, la vérification si la prestation sollicitée est qualifiée d'accident (art. 10 ss LAA et art. 9 ss OLAA) et donc aussi la décision quant à un droit éventuel est automatisée. Cela ne donne lieu à aucun profilage, puisque seules les factures sont contrôlées sur la base des données selon les contrats et les tarifs. Dans la mesure où une action en recouvrement de créance a été engagée, les autres démarches (réquisition de continuer la poursuite, réquisition de faillite, réquisition de réalisation, etc.) sont automatisées, pour autant qu'elles aient été engagées après l'expiration du délai correspondant, si la créance n'a pas encore été réglée. De telles décisions individuelles automatisées sont prises, parce qu'elles sont néces-

saires à l'exécution du contrat d'assurance entre le client et Helsana et qu'il existe des mesures appropriées pour que les droits et les intérêts légitimes des personnes concernées soient préservés (cf. ch. 11).

5. But et cadre légal du traitement des données

5.1 Données des clients

Les données de clients sont avant tout collectées pour la bonne exécution de l'assurance-accidents obligatoire conformément aux finalités légales suivantes (art. 96 LAA) :

- respect de l'obligation de s'assurer ;
- calcul et perception des primes ;
- établissement du droit aux prestations, calcul, allocation et coordination avec celles d'autres assurances sociales ;
- exercice d'une prétention récursoire contre le tiers responsable (recours) ;
- établissement des statistiques ;
- attribution ou vérification du numéro d'assuré AVS ;
- communication à des tiers selon les art. 97 et 98 LAA.

Par ailleurs, les traitements de données ont notamment (aussi) les buts suivants, pour autant que la loi le permette :

- protection des clients, collaborateurs et d'autres personnes, notamment dans des cas de menaces concernant des collaborateurs et protection des données, secrets et valeurs patrimoniales confiés à Helsana, sécurité des systèmes et des bâtiments d'Helsana ;
- en relation avec les prestations proposées, conclusion de contrats, gestion des contrats, entretien et développement des relations clients, communication, service Clientèle et assistance, promotions, publicité et marketing (y compris la newsletter et l'envoi de supports publicitaires) ;
- gestion, exploitation et développement du site Internet (y compris la mise à disposition de fonctions qui supposent des identificateurs ou d'autres données personnelles) et d'autres systèmes informatiques, vérifications d'identité ;
- respect des exigences légales et réglementaires et des règles internes d'Helsana, poursuite et mise en œuvre de différents droits, défense contre les prétentions juridiques, procédure civile, recours, lutte contre les abus, aux fins des enquêtes ou procédures légales et pour répondre aux demandes des autorités ;
- vente ou achat de domaines d'entreprise, de sociétés ou de parts de sociétés et autres transactions relevant du droit des sociétés et la transmission correspondante de données de clients ;
- à d'autres fins, pour autant qu'une obligation légale requière le traitement ou que celles-ci aient été identifiables ou indiquées au vu des circonstances à la date de collecte des données,

et dans le domaine des clients Entreprises pour

- le contrôle de la qualité, les études de marché, le développement de produits et de prestations, l'établissement de statistiques, les budgets, enregistrements et informations du management et autres rapports sur des clients, des transactions et des activités, offres et autres aspects com-

merciaux d'Helsana aux fins de la gestion et du développement de l'entreprise, de son offre et de ses activités, gestion de projets ;

(qualifiés ensemble de **finalité du traitement des clients**).

Helsana utilise les données des clients pour la finalité du traitement des clients en vertu du cadre légal suivant :

- exécution du contrat ;
- exécution d'une obligation légale d'Helsana ;
- consentement du client (notamment si un traitement est effectué en réponse à une demande concrète qui peut être retirée en tout temps, notamment pour la réception de newsletters auxquelles le client s'est abonné) ;
- intérêts légitimes d'Helsana, notamment
    - protection efficiente et effective des clients, collaborateurs et autres personnes et protection des données, secrets et valeurs patrimoniales d'Helsana et de ceux qui lui ont été confiés, sécurité des systèmes et des bâtiments d'Helsana ;
    - respect des exigences légales et réglementaires et des règles internes d'Helsana ;
    - suivi effectif et efficient de la clientèle, entretien des contacts et autre communication avec des clients, même en dehors de l'exécution des contrats ;
    - maintien et organisation sûre, efficiente et effective de l'activité, y compris d'une exploitation sûre, efficiente et effective et d'un développement réussi du site Internet et d'autres systèmes informatiques ;
    - vente et livraison de produits et de prestations, même en relation avec des personnes qui ne sont pas directement des cocontractants (p. ex. bénéficiaires) ;
    - gestion et développement pertinents de l'entreprise ;
    - suivi du comportement, des activités, de la situation et des besoins des clients, études de marché ;
    - amélioration efficiente et effective des produits et prestations existants et développement de nouveaux produits et prestations ;
    - réalisation de la publicité et du marketing ;
    - exploitation des systèmes informatiques d'Helsana ;
    - vente ou achat réussi de domaines d'entreprise, de sociétés ou de parts de sociétés et autres transactions relevant du droit des sociétés ;
    - intérêt pour la prévention des fraudes, délits et crimes ainsi que pour les enquêtes en relation avec de tels délits et autres comportements inappropriés, traitement des actions et procédures juridiques à l'encontre d'Helsana, participation à des procédures judiciaires et coopération avec les autorités et par ailleurs, revendication, exercice ou défense de prétentions juridiques.

5.2 Données des partenaires

Helsana peut traiter les données des partenaires notamment aux fins suivantes, pour autant que le droit de la protection des données applicables le permette : la conclusion et l'exécution de contrats et d'autres relations commerciales avec des partenaires, promotions, publicité et marketing, communica-

tion, invitation à des manifestations et participation à des actions pour les partenaires, réalisation d'activités communes, respect des exigences légales et réglementaires et des règles internes d'Helsana, poursuite et mise en œuvre de différents droits, défense contre les prétentions juridiques, procédure civile, recours, lutte contre les abus et les fraudes, aux fins des enquêtes ou procédures légales et pour répondre aux demandes des autorités, pour la vente ou l'achat de domaines d'entreprise, de sociétés ou de parts de sociétés et autres transactions relevant du droit des sociétés et la transmission correspondante de données de partenaires. Elle le fait sur la même base que pour les données des clients, conformément aux explications ci-dessus.

6. Communication de données à des tiers

6.1 Obligation de garder le secret

Tous les collaborateurs d'Helsana sont soumis à l'obligation de garder le secret (art. 33 LPGA). Les collaborateurs ont été informés des sanctions et signent en outre une déclaration d'obligation de garder le secret et de devoir de discrétion à leur entrée chez Helsana.

6.2 Exceptions au devoir de discrétion

Les exceptions à l'obligation de garder le secret sont réglées par la loi (art. 32 LGPA en liaison avec les art. 97 et 98 LAA) et sont effectives, pour autant qu'aucun intérêt privé prépondérant ne s'y oppose, notamment pour le traitement des données personnelles par

- des tiers sur mandat d'Helsana ;
- d'autres tiers, pour autant qu'il y ait dans le cas particulier un consentement écrit de la personne concernée, que l'obtention d'un consentement soit impossible ou que le consentement puisse être supposé comme étant dans l'intérêt de la personne assurée au vu des circonstances ;
- d'autres organes de l'assurance sociale, pour autant que cela soit nécessaire pour l'exécution de leurs tâches légales ou qu'il existe une obligation légale de communication ;
- d'autres autorités, tribunaux et services officiels (p. ex. en relation avec les impôts à la source, la statistique fédérale, une plainte pénale et la prévention des crimes, l'encaissement des primes).

Les données non personnelles peuvent être communiquées, pour autant qu'elles répondent à un intérêt prépondérant. Si l'anonymat des personnes concernées est préservé, des données d'intérêt général peuvent être publiées.

6.3 Catégories de tiers

Pour autant que le droit (de protection des données) applicable le permette, Helsana peut transmettre des données de clients et de partenaires aux catégories de tiers suivantes, qui traitent les données personnelles pour la finalité de traitement respective sur mandat d'Helsana ou à leurs propres fins :

- personnes concernées (notamment assurés) et tiers mandatés par elles ;
- autres sociétés du Groupe Helsana ;
- autres assureurs(-maladie) en dehors du Groupe Helsana ;
- organisations de branche, fédérations, organisations et autres comités ;
- fournisseurs de prestations, médecins-conseils, office de médiation ;

- prestataires (à l'intérieur et à l'extérieur du Groupe Helsana) ; y compris les sous-traitants chargés du traitement ;
- fournisseurs et autres partenaires commerciaux ;
- acquéreurs ou acquéreurs potentiels de domaines d'entreprise, de sociétés ou d'autres parties d'Helsana ;
- médias ;
- public ;
- autorités et services officiels locaux, nationaux et étrangers (notamment organes de la Confédération et des cantons, offices AI, etc.) ;
- autres parties dans des procédures judiciaires éventuelles ou effectives.

7. Transmission de données à l'étranger

Helsana peut transmettre des données de clients et de partenaires à l'intérieur d'Helsana, mais aussi à des tiers dans n'importe quel pays du monde, notamment dans tous les pays dans lesquels les prestataires d'Helsana traitent ses données (notamment aux Pays-Bas, en Irlande et en Allemagne). Lorsque des données sont transmises dans un pays sans protection des données appropriée, Helsana assure une protection appropriée en utilisant suffisamment de garanties contractuelles, notamment sur la base des clauses contractuelles types de l'UE, des Binding Corporate Rules ou s'appuie sur les exceptions du consentement, de l'exécution du contrat, de la constatation, de l'exercice ou de de la satisfaction de prétentions juridiques, de l'intérêt public prépondérant, des données publiées par le client ou les partenaires ou parce que cela est nécessaire à la protection de l'intégrité de ces personnes. Le client et partenaire peut exiger une copie des garanties contractuelles par écrit à l'adresse de contact précitée en joignant une copie d'une pièce d'identité officielle (cf. ch. 3) ou apprend ainsi où une telle copie peut être demandée. Helsana se réserve le droit de caviarder de telles copies pour des raisons liées à la protection des données ou de confidentialité.

Des données sont transmises à l'étranger, notamment à des fournisseurs de prestations étrangers en lien avec des garanties de prise en charge des coûts, des formulaires E et des rapatriements.

8. Conservation des données

Helsana enregistre en principe les données de clients et de partenaires en relation avec le contrat pendant la durée de la relation contractuelle qui peut parfois durer jusqu'à l'âge de la retraite et pour les rentes d'invalidité LAA jusqu'au décès, et dix ans après la cessation des rapports contractuels, pour autant qu'il n'y ait pas dans le cas particulier d'obligations de conservation légales plus courtes ou plus longues, que cela soit obligatoire pour des raisons de preuve ou qu'il existe un autre motif d'exception selon le droit applicable ou qu'une suppression anticipée soit indiquée (notamment parce que les données ne sont plus requises ou qu'Helsana est tenue de les supprimer).

Des délais de conservation plus courts d'au plus 13 mois s'appliquent pour les données de l'entreprise qui contiennent des données de clients ou de partenaires (p. ex. procès-verbaux, journaux).

Les documents commerciaux, y compris la communication, sont conservés tant qu'Helsana possède un intérêt dans ce sens (notamment un intérêt en matière de preuve en cas de prétentions, de documentation du respect de certaines prescriptions légales et autres, un intérêt pour une analyse à des fins non personnelles) ou est tenue de le faire (contractuellement, légalement ou en raison d'autres prescriptions). Les obligations légales concernant par exemple l'anonymisation ou la pseudonymisation des données demeurent réservées.

9. Fichier d'Helsana

9.1 Structure

Le fichier d'Helsana est classé par activités de données et inclut les catégories suivantes :

- gestion des canaux de vente et soutien à la vente ;
- élaboration des offres ;
- affaires avec de nouveaux clients ;
- service Clients ;
- gestion des contrats ;
- gestion des prestations ;
- achat de prestations ;
- assurance du personnel ;
- sciences de la santé ;
- encaissement, finances, actuariat ;
- audit, Risk, Legal et Compliance ;
- gestion informatique et gestion de la sécurité des données ;
- fondation de prévoyance du personnel ;
- achat.

Différentes interfaces telles que MediData permettent un contact direct avec des prestataires et fournisseurs de prestations externes, par exemple en cas de décompte direct du fournisseur de prestations avec Helsana. Il existe par ailleurs une interface par le biais de laquelle certains fournisseurs de prestations peuvent contrôler en ligne la couverture d'assurance d'un assuré. La protection des données et la sécurité correspondante des données sont garanties grâce à une authentification forte, à une technologie de cryptage et de transmission moderne.

9.2 Utilisation et accès aux données

9.2.1 Détenteurs d'un droit d'accès

Ont le droit d'accéder au fichier d'Helsana :

- les collaborateurs d'Helsana, pour autant qu'ils en aient besoin pour exécuter leur mandat de « mise en œuvre de l'assurance-accidents » ;
- les administrateurs système d'Helsana ;
- les prestataires mandatés par contrat ;

(qualifiés tous ensemble de **détenteurs d'un droit d'accès**).

9.2.2 Gestion des détenteurs d'un droit d'accès

La gestion des détenteurs d'un droit d'accès est assurée de manière centralisée par Helsana. Les collaborateurs internes sont déclarés par le biais de l'interface des RH et les collaborateurs externes par le biais du sourcing respectif. De nouvelles identités, y compris les comptes correspondants, ne sont saisies que s'il existe un contrat de travail ou un contrat de prestations valables et une validation correspondante des droits par le supérieur hiérarchique.

9.2.3 Droit d'accès personnel

A son entrée chez Helsana, chaque détenteur d'un droit d'accès reçoit ses droits d'accès pour information, conformément au modèle de rôles et sur la base de sa fonction. Tous les autres droits requis doivent être demandés individuellement par le biais du portail d'autorisation. On considère à ce sujet que chaque demande doit être confirmée par le supérieur direct et, selon le rôle d'autorisation, aussi par l'approbateur des rôles.

9.2.4 Annulation du droit d'accès

Les détenteurs d'un droit d'accès du fichier d'Helsana n'ont un droit d'accès que tant qu'ils ont besoin des données pour l'exercice de leur fonction. En cas de départ ou de changement d'attribution au sein d'Helsana, le droit d'accès est retiré et les droits d'accès requis pour les nouvelles attributions sont réaffectés par le biais du modèle de rôles.

9.2.5 Formation des détenteurs d'un droit d'accès

Des cours sont dispensés aux détenteurs d'un droit d'accès afin de les former aux différents sous-systèmes et applications.

9.2.6 Manuels et directives de traitement pour les détenteurs d'un droit d'accès

Il existe des documents correspondant aux sous-systèmes. Le traitement des données est par ailleurs fixé dans des directives, des règlements et des manuels de prestations ainsi que dans des listes. Ils sont régulièrement mis à jour par les unités d'organisation compétentes.

Grâce à des instructions spécifiques, celles-ci instaurent un niveau constant d'évaluation des prestations selon la LAA pour l'ensemble du territoire d'assurance de la Suisse, grâce à des instructions spécifiques.

9.2.7 Prestataires informatiques

Dans la mesure où l'exploitation du fichier d'Helsana est externalisée à des prestataires informatiques externes, ceux-ci respectent des réglementations similaires dans leur domaine.

10. Mesures techniques et organisationnelles

10.1 Contrôle d'accès

Tous les locaux d'Helsana dans lesquels sont traitées des données personnelles sensibles sont protégés contre les accès de personnes non autorisées, soit manuellement, soit électroniquement. Les responsables journalisent la gestion des clés et le contrôle d'accès électronique. Le mandataire à la sécuri-

té physique peut en tout temps exiger de consulter le journal ou des analyses. Les mesures de sécurité sont déterminées par des zones de protection : les places de travail sont protégées contre l'accès par des tiers non autorisés. Les locaux spéciaux et les pièces sensibles telles que les locaux techniques et les centres de calcul sont sécurisés comme suit :

- les supports de données électroniques dans les centres de calcul exploités par le service informatique d'Helsana et les serveurs décentralisés exploités par le service informatique d'Helsana sont sécurisés exclusivement pour l'accès de personnes autorisées spécifiques, grâce à des exigences de sécurité physiques 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 à celles qu'il met lui-même en œuvre.

10.2 Contrôle des supports de données personnelles

Grâce à des précautions techniques, seules les personnes autorisées ont la possibilité de traiter des données sur les supports de données électroniques. Seules les personnes autorisées ont accès au fichier d'Helsana.

10.3 Authentification des détenteurs d'un droit d'accès

L'accès aux sous-systèmes du fichier d'Helsana est protégé par l'ID d'utilisateur combinée avec un mot de passe individuel d'une durée déterminée.

10.4 Contrôle de communication

Les destinataires de données à qui des données personnelles sont communiquées à l'aide d'équipements de transmission de données sont identifiés par le biais des interfaces (p. ex. consultations de la couverture en ligne par les fournisseurs de prestations en relation avec l'utilisation de la carte d'assuré).

10.5 Transmission des données

La transmission des données entre les terminaux de données et les ordinateurs hôtes est protégée par le protocole de transfert.

10.6 Contrôle de mémoire

Les détenteurs d'un droit d'accès reçoivent des autorisations spécifiques concernant les modifications dans des champs de données, dont ils ont besoin pour exécuter leurs tâches selon la LAA.

10.7 Exigences techniques à l'égard des terminaux

L'accès au réseau interne d'Helsana est restreint, protégé et surveillé grâce à des mesures de contrôle spécifiques. Des précautions similaires existent chez les prestataires informatiques externes pour leurs réseaux.

10.8 Mesures en vue de la protection des données (confidentialité) dans le domaine des terminaux

Les terminaux de données sont disposés dans des zones protégées. Les terminaux mobiles contiennent des mémoires protégées par un procédé de cryptage fort, basé sur 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. En application d'une directive interne, ces données sont soit conservées dans des conteneurs verrouillables, soit éliminées à l'aide de destructeurs de documents ou de Datarec.

10.9 Journalisation

En plus du contrôle des accès au fichier d'Helsana par le biais de la procédure d'autorisation ainsi que de la protection de l'ID d'utilisateur personnelle et de l'identification par mot de passe, certains sous-systèmes disposent d'une journalisation du traitement automatisé, afin de pouvoir vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. La journalisation est réalisée en application de l'art. 10 OLPD. Les procès-verbaux de journalisation sont conservés durant 13 mois et sous une forme répondant aux exigences de la révision. Ils sont accessibles aux seuls organes chargés de vérifier l'application des dispositions de protection et de sécurité des données personnelles, et ils ne sont utilisés qu'à cette fin. Il existe parfois des réglementations similaires mais spécifiques en matière de journalisation chez les prestataires informatiques externes.

10.10 Développement

Les demandes de développement du système sont regroupées et définies, budgétisées et réalisées sous forme de maintenance, de petit projet ou de projet. La procédure est réglée dans le cadre de la « gestion de projets Helsana ».

10.11 Soutien aux détenteurs d'un droit d'accès et obligation de déclarer

Au plan technique, les détenteurs d'un droit d'accès sont soutenus par les services spécialisés de la direction des domaines correspondants. L'assistance technique pour les terminaux de données et le réseau est assurée par le service informatique d'Helsana ou sous-traitée.

Les détenteurs d'un droit d'accès sont informés sur le niveau de sécurité du fichier d'Helsana et les prescriptions en matière de gestion du système et de ses données. Les dispositions sont décrites dans les manuels d'exploitation à la rubrique Sécurité de l'information. Les sanctions éventuelles en cas de manquements délibérés ou par négligence à la sécurité de l'information sont connues des détenteurs d'un droit d'accès.

Tous les détenteurs d'un droit d'accès sont tenus de déclarer les constatations suivantes au responsable du processus ou représentant des détenteurs d'un droit d'accès :

- faiblesses ou problèmes de sécurité du système observés ou supposés ;
- mesures de sécurité non appliquées ou non respectées ;
- événements imprévus susceptibles d'avoir une incidence sur la sécurité de l'information.

10.12 Surveillance et responsabilité

Les responsables du processus des sous-systèmes surveillent le respect des directives et du présent règlement de traitement des données par les détenteurs d'un droit d'accès et de leurs prescriptions contractuelles par les prestataires informatiques externes.

11. Droits des clients et partenaires

Chaque personne concernée, client et partenaire, dispose vis-à-vis d'Helsana d'un droit d'accès à ses données personnelles. Elle a en outre le droit d'exiger d'Helsana la correction, la suppression et la limitation de ses données personnelles et de s'opposer à un tel traitement des données personnelles. Si le traitement des données se fonde sur un consentement, la personne concernée peut en tout temps le révoquer. Dans des Etats de l'UE ou de l'EEE, la personne concernée a le droit, dans certains cas, de recevoir les données générées par l'utilisation de services en ligne dans un format structuré, courant et lisible par machine, qui permet une utilisation et une transmission ultérieures. Les demandes en relation avec ces droits doivent être adressées par écrit à l'adresse de contact en joignant une copie d'une pièce d'identité officielle (cf. ch. 3). Helsana se réserve le droit de restreindre les droits de la personne concernée dans le cadre du droit applicable correspondant et p. ex. de ne pas fournir de renseignement complet ou de ne pas supprimer des données.

Si Helsana prend de manière automatique une décision concernant une personne qui a des conséquences juridiques sur la personne en question ou qui constitue pour elle une entrave importante, de façon similaire, la personne concernée peut s'entretenir avec une personne compétente chez Helsana et exiger de sa part un nouvel examen de la décision ou exiger d'emblée une évaluation par une personne, pour autant que le droit applicable le prévoie. Dans ce cas, la personne concernée ne peut éventuellement plus utiliser certaines prestations automatisées. La personne est informée de telles décisions, ultérieurement ou préalablement de manière séparée.

Chaque personne concernée a le droit de former un recours auprès de l'autorité compétente en matière de protection des données. En Suisse, il s'agit du Préposé fédéral à la protection des données et à la transparence (http://www.edoeb.admin.ch).

12. Modification de la déclaration de protection des données

Helsana peut adapter la présente déclaration de données en tout temps, sans préavis ni notification. La version actuelle publiée sur le site Internet s'applique.

Dans la mesure où la déclaration de protection des données fait partie d'un accord avec les clients et partenaires, Helsana peut les informer de la modification par courriel ou de toute autre manière appropriée en cas de mise à jour. En l'absence de contestation dans les 30 jours, la nouvelle déclaration de protection des données est réputée convenue. En cas de contestation, Helsana peut procéder à la résiliation extraordinaire et immédiate de la convention.

* * * * *