Fondation Agrisano
Caisse-maladie Agrisano SA
Assurances Agrisano SA
Agrisano Pencas
Agrisano Prevos

Directives sur la protection des données

Fondation Agrisano
Caisse-maladie Agrisano SA
Assurances Agrisano SA
Agrisano Pencas
Agrisano Prevos

Laurstrasse 10 | 5201 Brugg | Téléphone +41 56 461 71 11
info@agrisano.ch | agrisano.ch

Sommaire

1. Dispositions générales 4
1.1. Bases légales et champ d'application 4
1.2. Responsabilités au sein des entreprises Agrisano 4
1.3. Confidentialité et obligation de garder le secret 4
1.4. Conseillère/conseiller à la protection des données et contact pour les questions relatives à la protection des données 5
1.5. Données personnelles 5
1.6. Principes du traitement 6
2. Organisation et charte de protection des données 6
2.1. Secrétariat d'Agrisano 6
2.2. Agences régionales d'Agrisano 6
2.3. Organigrammes 6
3. Accès aux données, utilisatrices et utilisateurs 7
3.1. Principe 7
3.2. Droits des utilisatrices/utilisateurs et gestion des utilisatrices/utilisateurs 7
3.3. Droit d'accès personnel / authentification de l'utilisatrice/utilisateur 7
3.4. Suppression des droits d'accès 7
4. Autres obligations du responsable (Agrisano) 8
4.1. Déclaration des fichiers et annonce des répertoires de traitement au PFPDT 8
4.2. Annonce des violations de la protection des données au PFPDT 8
5. Mesures techniques et organisationnelles garantissant la sécurité des données 9
5.1. Principes 9
5.2. Structure informatique 9
5.3. Contrôle d'accès (accès au bâtiment) 9
5.4. Authentification 10
5.5. Contrôles et procès-verbaux 10
5.6. Autres mesures concrètes de protection des données 11
5.7. Mesures organisationnelles de protection des données 11
5.8. Protection de la vie privée dès la conception et protection de la vie privée par défaut 11
6. Traitement des données 12
6.1. Traitement par un sous-traitant 12
6.2. Objectif du traitement de données 12

6.3. Type de données 12
6.4. Registre des activités de traitement 13
6.5. Documentation des fichiers 13
6.6. Provenance des données 13
6.7. Catégories de données 14
6.8. Transmission des données 15
6.9. Profilage et décisions individuelles automatisées 15
6.10. Transfert de données à l'étranger 15
6.11. Réseaux sociaux 15
6.12. Archivage et destruction 16
6.13. Service de réception des données (SRD) dans le domaine du traitement électronique 16
7. Droit d'accès, de rectification et de remise 16
7.1. Droit d'accès 16
7.2. Remise des données et consultation des dossiers 16
7.3. Rectification des données personnelles / interdiction de communiquer et de traiter des données 17
8. Gestion de la qualité et système de contrôle interne 18
9. Publication, entrée en vigueur, application et modifications 18
10. Abréviations utilisées dans le présent document 19

1. Dispositions générales

1.1. Bases légales et champ d'application

Ces directives sur la protection des données se basent sur la loi sur la protection des données (LPD) totalement révisée, les dispositions d'exécution de la nouvelle ordonnance sur la protection des données (OPD) et la nouvelle ordonnance sur les certifications en matière de protection des données (OCPD), entrée en vigueur au 1er septembre 2023.

La loi révisée sur la protection des données se limite à la protection des données des personnes physiques et ne s'applique donc plus aux données des personnes morales. La loi s'applique au traitement des données personnelles par les particuliers et les organes fédéraux.

Les caisses-maladie sont considérées comme des organes fédéraux dans le domaine de la loi sur l'assurance maladie (LAMal) et comme des responsables de traitement privés dans le domaine de la loi sur le contrat d'assurance (LCA). La Caisse-maladie Agrisano SA gère l'assurance obligatoire des soins (AOS) et est donc considérée comme un organe fédéral.

Les caisses de pension et les fondations de prévoyance sont considérées comme des organes fédéraux lorsqu'elles sont actives, entièrement ou partiellement, dans le domaine obligatoire. En raison de la partie obligatoire, Agrisano Pencas est donc considérée comme un organe fédéral. Agrisano Prevos compte, avec la Fondation Agrisano et Agrisano Assurances SA, parmi les personnes privées. Les normes spécifiques de protection des données (p. ex. l'art. 86a LPP) priment sur celles de la LPD.

Les processus de traitement des données sont identiques dans toutes les entreprises Agrisano.

1.2. Responsabilités au sein des entreprises Agrisano

La responsabilité globale de la protection des données incombe à l'organe de direction de l'entreprise Agrisano concernée. Cette responsabilité est intransmissible.

La conseillère/le conseiller en protection des données est responsable de la mise en œuvre de la protection des données dans l'entreprise. Elle ou il veille au respect de la protection des données, conseille la direction et le personnel et les assiste dans la mise en œuvre opérationnelle de la protection des données dans l'entreprise.

Agrisano exploite ses systèmes informatiques avec sa propre équipe informatique interne. L'équipe IT-Operations se compose de six personnes (avec des droits d'accès et d'entrée spéciaux) et est responsable de l'ensemble de l'exploitation et de l'infrastructure.

1.3. Confidentialité et obligation de garder le secret

Collaboratrices et collaborateurs

Dans l'accomplissement de leurs tâches au moyen des systèmes informatiques, les collaboratrices et collaborateurs d'Agrisano traitent des données personnelles.

Agrisano accorde une grande importance à la protection des données, se conforme à la législation en la matière et règle la protection des données dans différents documents accessibles à l'ensemble du personnel. L'ensemble des collaboratrices et collaborateurs sont soumis au secret professionnel conformément à l'art. 33 de la Loi fédérale sur la partie générale du droit des assurances sociales (LPGA) et 62 de la Loi fédérale sur la protection

des données (LPD) et s'engagent, par la signature de leur contrat de travail, à garder le secret, à ne divulguer aucune information et à respecter la législation sur la protection des données.

Partenaires externes

Des contrats de collaboration ont été conclus avec les partenaires externes des entreprises Agrisano. Ces partenaires s'engagent contractuellement à respecter les dispositions de protection des données dans la même étendue qu'Agrisano.

1.4. Conseillère/conseiller à la protection des données et contact pour les questions relatives à la protection des données

Les entreprises privées (donc la Fondation Agrisano, Agrisano Assurances SA et Agrisano Prevos) peuvent nommer une conseillère ou un conseiller à la protection des données (CPD); les organes fédéraux (Caisse-maladie Agrisano SA et Agrisano Pencas) ont l'obligation légale de le faire. Dans ce cas, la conseillère ou le conseiller à la protection des données ne représente pas seulement un point de contact interne à l'entreprise, mais aussi un lien avec la protection des données des autorités et la première personne de contact du Préposé fédéral à la protection des données et à la transparence (PFPDT).

Pour toutes les questions et demandes en rapport avec la protection des données (en particulier le traitement des demandes de renseignements de la part de tiers, le contrôle de la communication de données personnelles à des tiers et le traitement et l'examen des violations de la protection des données), le service suivant peut être contacté dans toutes les entreprises Agrisano:

Agrisano
Conseiller/ère à la protection des données
Laurstrasse 10
5201 Brugg
Tél. +41 56 461 71 11 / E-mail: datenschutz@agrisano.ch

Les demandes concernant la protection des données doivent être adressées par écrit à l'adresse ci-dessus, accompagnées d'une copie d'une pièce d'identité (afin de vérifier l'identité et d'exclure tout abus).

1.5. Données personnelles

La LPD révisée vise exclusivement à protéger la personnalité des personnes **physiques** dont des données personnelles sont traitées. Elle ne concerne pas les données des personnes morales telles que les sociétés commerciales, les associations ou les fondations.

Sont considérées comme données personnelles toutes les données qui se rapportent à une personne et qui l'identifient ou contribuent à son identification. La loi sur la protection des données opère une distinction entre les **données personnelles** et les **données personnelles sensibles**. En principe, toutes les données personnelles sont dignes de protection. Il y a des exigences supplémentaires en ce qui concerne le traitement des données personnelles sensibles.

Selon la LPD, les **données personnelles sensibles** sont:

- les informations sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales;
- les données relatives à la santé, à la sphère intime ou à l'appartenance à une race ou à une ethnie;
- les données génétiques;
- les données biométriques qui permettent d'identifier clairement un individu;
- les données relatives aux poursuites administratives et pénales ou aux sanctions;
- les données sur les mesures d'aide sociale.

* Les données suivantes, en particulier, peuvent contenir des informations sur la santé d'une personne : enregistrement du déroulement d'un traitement, description des symptômes, diagnostics, ordonnances / rapports médicaux / rapports d'hôpitaux, thérapies, médicaments, transferts, résultats de laboratoire, positions tarifaires, enregistrements de procédures d'imagerie.

1.6. Principes du traitement

- Agrisano garanti que tout traitement de données personnelles est licite.
- Le traitement de l'Agrisano des données personnelles est conforme aux principes de la bonne foi et de la proportionnalité.
- Les données personnelles ne sont collectées qu'aux fins de la relation d'assurance et reconnaissables pour la personne concernée et sont traitées ultérieurement de manière compatible avec ces finalités.
- Les données personnelles sont détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement.
- Agrisano s'assure que les données personnelles traitées sont exactes.

2. Organisation et charte de protection des données

2.1. Secrétariat d'Agrisano

Les cinq entreprises Agrisano emploient environ 290 personnes (état : avril 2023 / Assurances Agrisano SA ne dispose pas de son propre personnel).

2.2. Agences régionales d'Agrisano

Agrisano est en étroite collaboration avec les organisations professionnelles agricoles cantonales, qui gèrent pour Agrisano des agences régionales (offices régionaux).

Ces agences régionales disposent de leur propre infrastructure informatique et accèdent exclusivement aux systèmes et programmes nécessaires via une connexion sécurisée avec Agrisano.

2.3. Organigrammes

Les organigrammes actuels se trouvent sur notre site Internet, à la rubrique « En un coup d'œil » (Entreprises – Agrisano – Union suisse des paysans).

3. Accès aux données, utilisatrices et utilisateurs

3.1. Principe

Les utilisatrices et utilisateurs n'ont accès qu'aux données, programmes et fonctions qui leur sont nécessaires pour exercer leur activité (elles et ils sont regroupés en fonction de leurs tâches). Les droits d'accès des groupes dépendent de la fonction et des domaines d'activité (y compris la distinction entre droit de lecture et droit de modification).

Ils existent des directives séparées pour l'utilisation générale de l'installation informatique.

3.2. Droits des utilisatrices/utilisateurs et gestion des utilisatrices/utilisateurs

L'attribution des droits d'accès est liée à la fonction concernée et réglée par un concept d'autorisation. Les autorisations supplémentaires pour une fonction qui s'écartent du concept d'autorisation ne peuvent être demandées que par le propriétaire des données concerné. Toutes les autorisations (y compris les droits d'utilisation privilégiés) sont soumises à un contrôle annuel par les propriétaires de données.

3.3. Droit d'accès personnel / authentification de l'utilisatrice/utilisateur

Les systèmes informatiques d'Agrisano ne peuvent être utilisés qu'avec le nom d'utilisatrice/utilisateur personnel et le mot de passe correspondant (la complexité du mot de passe est réglée séparément). Il est interdit de transmettre son mot de passe personnel à autrui. La complexité du mot de passe est en outre contrôlée au niveau du système et le changement de mot de passe est également exigé à intervalles réguliers.

L'accès à l'infrastructure informatique d'Agrisano depuis l'extérieur (par exemple en télétravail) est exclusivement possible via un tunnel IPSec ou un client VPN avec authentification à deux facteurs.

3.4. Suppression des droits d'accès

Les droits d'accès au système informatique d'Agrisano ne sont valables que pour la durée des rapports de travail. En cas de départ, les droits d'accès sont retirés ; en cas de nouvelles responsabilités au sein d'Agrisano, ils sont attribués en fonction du nouveau domaine d'activité.

4. Autres obligations du responsable (Agrisano)

4.1. Déclaration des fichiers et annonce des répertoires de traitement au PFPDT

Avec l'entrée en vigueur de la nouvelle loi sur la protection des données (LPD), la déclaration des fichiers au registre du PFPDT est modifiée. À partir de cette date, seuls les organes fédéraux (donc Agrisano Caisse-maladie SA et Agrisano Pencas) doivent déclarer leurs fichiers (désormais : indiquer au PFPDT les inscriptions du registre des activités de traitement selon l'art. 12 LPD). Les organismes privés (Fondation Agrisano, Assurances Agrisano SA et Agrisano Prevos) ne sont pas concernés par cette obligation.

Le PFPDT publie les communications des organes fédéraux dans un registre accessible au public, le DataReg. Le conseiller/la conseillère à la protection des données est responsable de la mise à jour du registre.

4.2. Annonce des violations de la protection des données au PFPDT

Les violations de la sécurité des données, c'est-à-dire la perte, l'effacement, la destruction, la modification ou la mise à disposition non autorisée de données personnelles, que ce soit par inadvertance ou de manière illicite, doivent être annoncées au PFPDT le plus rapidement possible lorsqu'elles sont susceptibles d'entraîner un risque élevé pour les personnes concernées (violation de la sécurité des données).

Pour ce faire, un service en ligne d'annonce de violation de la sécurité des données est disponible sur le site Internet du PFPDT.

En règle générale, là ou le responsable doit également informer la ou les personne(s) concernée(s) si cela est nécessaire pour leur protection ou si le PFPDT l'exige.

La procédure et le processus d'annonce sont réglés séparément et s'appliquent à toutes les entreprises Agrisano ainsi qu'aux agences régionales.

5. Mesures techniques et organisationnelles garantissant la sécurité des données

5.1. Principes

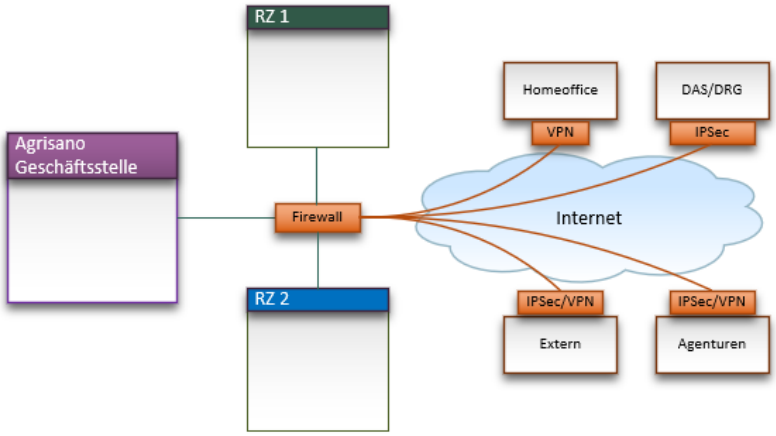
Diverses mesures techniques et organisationnelles permettent de garantir une sécurité adéquate des données. Il est tenu compte des objectifs suivants, conformément au règlement sur la protection des données. Les données:

- ne sont accessibles qu'aux personnes autorisées (confidentialité) ;
- sont disponibles lorsqu'elles sont nécessaires (disponibilité) ;
- ne sont pas modifiées sans autorisation ou par inadvertance (intégrité) ;
- sont traitées de manière compréhensible (traçabilité).

5.2. Structure informatique

Agrisano dispose de deux centres de calcul décentralisés qui sont particulièrement protégés par différents dispositifs techniques (par ex. alimentation électrique sans interruption, climatisation, système de détection d'incendie, alarme, etc.) et dont l'accès est réservé à des personnes spécialement autorisées. Les serveurs exploités par Agrisano-IT sont également équipés conformément à ces exigences de sécurité élevées.

La représentation graphique illustre la structure informatique, y compris la connexion des postes et des utilisatrices et utilisateurs depuis l'extérieur via un tunnel IPSec/VPN :



5.3. Contrôle d'accès (accès au bâtiment)

Au siège principal d'Agrisano, tous les locaux dans lesquels des données personnelles sont traitées sont protégés électroniquement et mécaniquement contre l'accès par des personnes non autorisées. Le système de fermeture électronique au siège (avec clé personnelle, appelée « badge ») se base sur une gestion des utilisatrices et utilisateurs propre. Les badges sont personnels ; il est interdit de les confier à d'autres collaboratrices ou collaborateurs ou à des tiers.

Les locaux particulièrement sensibles, par exemple ceux du groupe stationnaire ou le domaine SMC, sont séparés physiquement. Les locaux techniques et les centres de calcul sont en outre spécialement sécurisés (y

compris par un accès limité et des systèmes de sécurité séparés). Les droits d'accès aux archives sont également gérés de manière restrictive.

5.4. Authentification

Différentes mesures (p. ex. respect du concept d'autorisation, gestion/attribution de l'autorisation par les administrateurs système, directive sur les mots de passe, etc.) garantissent que les personnes autorisées ne peuvent accéder qu'aux données validées sur la base de leurs droits d'accès. Pour les autres règlements d'authentification, se référer au chiffre 3.

5.5. Contrôles et procès-verbaux

Contrôles

- **Contrôle de communication**
  Les destinataires à qui des données personnelles sont communiquées au moyen de dispositifs de transmission des données sont identifiées via les interfaces ou les connexions sécurisées.
- **Contrôle de mémoire**
  Les utilisatrices et utilisateurs reçoivent des autorisations spécifiques pour les mutations dans les champs de données qui leur sont nécessaires pour accomplir leurs tâches (p. ex. selon la LAMal).

Procès-verbaux

Les accès aux systèmes informatiques d'Agrisano sont limités autant que possible par le biais du concept d'autorisation des utilisatrices et utilisateurs (la suppression de données personnelles requiert par exemple le niveau d'autorisation le plus élevé). Comme l'utilisation des applications se fait toujours par le biais de l'ID utilisateur personnel et de l'autorisation, le traitement des données personnelles est également historisé (aucun procès-verbal n'est établi pour l'ensemble des modifications effectuées ; une consultation individuelle de la banque de données est effectuée sur demande).

Les accès des prestataires de services externes ou des personnes chargées du traitement des mandats sont sécurisés et historisés. Des règles internes en matière de journalisation s'appliquent.

5.6. Autres mesures concrètes de protection des données

Voici les principales mesures d'ordre technique :

- **Transmission des données** (p. ex. e-mails) par processus de cryptage ;
- **Exigences techniques appliquées aux terminaux :** limitation de l'accès au réseau interne d'Agrisano, l'accès externe se faisant par VPN ;
- **Sauvegarde des données :** sauvegarde ainsi que mise en miroir des systèmes de stockage sur différents sites ;
- **Sécurité informatique :** pare-feu, protection des terminaux et filtre contre les spams ;
- **Sécurité des systèmes :** les systèmes d'exploitation et les logiciels d'application sont toujours maintenus à jour en matière de sécurité et les failles connues sont rapidement comblées.

5.7. Mesures organisationnelles de protection des données

Les collaboratrices et collaborateurs d'Agrisano ont pour consigne de verrouiller leur écran lorsqu'ils quittent leur poste de travail (ceci s'applique également au télétravail).

Les données imprimées sont conservées de manière que des tiers (p. ex. le personnel d'entretien des locaux) ne puissent pas les consulter ou les copier.

Diverses directives internes s'appliquent au traitement des données personnelles sensibles, p. ex. concernant la conservation dans des contenants verrouillables, la destruction des documents via le système d'élimination de l'entreprise DataEx 4000, etc.

Agrisano applique le principe du « bureau propre » et de « l'écran propre ».

5.8. Protection de la vie privée dès la conception et protection de la vie privée par défaut

La protection de la vie privée dès la conception et la protection de la vie privée par défaut sont explicitement ancrées par les dispositions de l'article 7 de la loi sur la protection des données.

Lors du traitement de données personnelles, des mesures techniques et organisationnelles appropriées doivent être prises dès la conception du traitement pour garantir la mise en œuvre des principes de protection des données (p. ex. minimisation des données) dans ces systèmes (protection de la vie privée dès la conception). Les paramètres par défaut, par exemple pour les applications ou les sites Internet, doivent également être conçus de manière à ce que le traitement des données personnelles soit limité au minimum requis pour l'utilisation prévue (protection de la vie privée par défaut).

6. Traitement des données

6.1. Traitement par un sous-traitant

Conformément à l'art. 9 LPD, le traitement de données personnelles peut être confié à un sous-traitant par contrat ou par la législation, à condition que les données soient traitées comme le responsable devrait le faire lui-même et qu'aucune obligation légale ou contractuelle de confidentialité n'en interdise la délégation.

Les entreprises Agrisano collaborent au sein du groupe et avec des tiers.

6.2. Objectif du traitement de données

Agrisano traite les données exclusivement dans le but de réaliser ses activités d'assurance et les solutions de prévoyance qu'elle propose, en particulier pour la documentation des rapports d'assurance et de prévoyance, l'examen des propositions, le traitement des prestations, l'examen des limitations, le traitement des paiements ainsi que pour la tenue de statistiques et la fourniture de renseignements. Les données sont donc traitées exclusivement dans le cadre de l'exécution des droits et obligations légaux.

En outre, dans le cadre de l'activité commerciale générale, des données de fournisseurs de prestations, de prestataires, de fournisseurs, d'entreprises partenaires, de banques, d'autorités et d'administrations, etc., sont traitées. En règle générale, il s'agit toutefois de données de personnes morales, qui ne sont plus explicitement soumises à la loi sur la protection des données.

6.3. Type de données

Données personnelles et données clientèle : données de base et relatives à l'effectif (p. ex. prénom/nom, adresse, nationalité, date de naissance, état civil, numéro AVS et numéro d'assuré, langue, canton et commune d'appartenance, numéro de téléphone, adresse électronique, membres de la famille, personnes autorisées, coordonnées bancaires et informations de paiement).

Données de communication : toutes les données relatives aux communications personnelles, téléphoniques et écrites (courrier postal et électronique), aux demandes de contact via le site Internet, les données d'enquête, les newsletters, etc.

Données de la proposition : données en rapport avec les demandes d'offres ou les demandes d'adhésion (p. ex. données personnelles, modèles d'assurance souhaités, déclarations de santé).

Données relatives aux contrats de prévoyance ou d'assurance et aux primes (contrats individuels et collectifs): type d'assurance, conclusion, durée, primes, franchises, sommes d'assurance, etc.

Données relatives aux prestations (y c. Case Management) : données des fournisseurs de prestations, telles que factures ou coûts, diagnostics, rapports médicaux, etc.

Données SMC : documents du service médecin-conseil, p. ex. droits aux prestations, diagnostics, expertises médicales.

Données relatives aux paiements et aux encaissements : données liées à la comptabilité, telles que les postes non soldés, les paiements et les facturations, les demandes de remboursement.

Données marketing : magazine clientèle, données sur les actions de marketing, résultats d'enquêtes auprès de la clientèle, participation à des concours (p. ex. coordonnées, préférences, besoins).

Données HR: données personnelles de base et données du dossier personnel (p. ex. dossiers de candidature, évaluations des collaboratrices et collaborateurs, certificats, formations et formations continues, horaires de travail, données de traitement des salaires).

Données de conformité et données relatives à la protection des données : données en rapport avec des évaluations de conformité ou des violations de la protection des données (informations sur les personnes concernées et impliquées).

Données relatives aux utilisatrices et utilisateurs et à l'utilisation du système et données techniques : données en relation avec la gestion des utilisatrices et utilisateurs (par ex. données personnelles, fonction, données d'accès), l'utilisation des systèmes informatiques ou du site Internet d'Agrisano (p. ex. numéros professionnels, adresses IP, identifiants internes et externes, enregistrements des accès).

Données provenant de la vidéosurveillance : fichiers d'images des caméras de surveillance à l'extérieur et dans le parking du siège principal d'Agrisano à Windisch.

6.4. Registre des activités de traitement

Conformément à l'art. 12 LPD, un registre des activités de traitement doit être tenu. Les indications nécessaires sont prescrites par la LPD. Ce registre a été établi par les entreprises Agrisano en 2023. Il est régulièrement complété et vérifié. De plus, il est actualisé sur base périodique.

Alors que les organes fédéraux (donc la Caisse-maladie Agrisano SA ainsi qu'Agrisano Pencas) doivent annoncer les répertoires au PFPDT, le nouveau droit ne prévoit plus d'obligation d'annonce pour les personnes privées traitant des données.

6.5. Documentation des fichiers

Les fichiers contenant des données personnelles sensibles des entreprises Agrisano sont documentés dans différents règlements, directives et instructions. Des documentations détaillées existent pour les processus dans lesquels des données personnelles sensibles sont traitées (notamment le service de réception des données DRG).

6.6. Provenance des données

Données transmises

Les données personnelles sont souvent communiquées à Agrisano par la personne concernée (p. ex. par le biais de formulaires, lors de la communication avec Agrisano, lors de l'utilisation de son site Internet, etc.) Si des contrats sont conclus avec Agrisano ou si des prestations sont demandées, différentes données sont transmises à Agrisano (p. ex. données personnelles de base, données relatives aux propositions ou données contractuelles).

Données reçues

Les données personnelles sont en partie transmises à Agrisano par des tiers, dont :

- les offices et registres publics (p. ex. contrôle des habitants, registre des poursuites, etc.) ou la poste suisse;
- les autorités, tribunaux, parties et autres tiers en relation avec des procédures administratives et judiciaires;

- les employeurs ;
- l'entourage (famille, conseillères et conseillers, représentantes et représentants juridiques, etc.), les personnes autorisées ;
- les banques et autres prestataires de services financiers, les assurances privées ou sociales, les institutions de prévoyance et de libre passage ;
- les hôpitaux, les médecins et les autres prestataires de services, les spécialistes, les personnes chargées des expertises ;
- les prestataires de service (p. ex. les agences) ;
- les personnes chargées du placement de personnel (p. ex. les agences de placement, les chasseuses et chasseurs de têtes).

6.7. Catégories de données

Le traitement des données dépend de la catégorie de données définie. Les catégories suivantes ont été définies en rapport avec la protection des données :

1	Données personnelles sensibles	Données relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales ; à la santé, à la sphère intime ou à l'appartenance à une race ou une ethnie, aux mesures d'aide sociale ; aux poursuites ou sanctions administratives et pénales et également aux données génétiques et biométriques. Le traitement de ces données exige le plus grand soin.
2	Données personnelles	Données qui selon la LPD, ne sont pas considérées comme « sensibles » par exemple les informations contenant le nom, le prénom et l'adresse ou une référence interne. Toutes les informations pouvant être associées à une personne physique identifiée ou identifiable.
3	Données factuelles	Les données qui ne permettent pas d'identifier de manière univoque une personne physique, ainsi que les données commerciales.
4	Données secrètes	Données personnelles sensibles, données relatives aux infrastructures (principe : need to know) : seuls les collaborateurs qui en ont besoin dans le cadre de leur activité y ont accès. Les échanges de courriels cryptés avec les assurés et les fournisseurs de prestations font également partie des données confidentielles. Les tiers ne peuvent consulter ces données que s'ils sont soumis à des obligations contractuelles de confidentialité. Les mots de passe des collaborateurs sont également confidentiels.
5	Données confidentielles	Données commerciales, données à caractère personnel et données à caractère personnel sensibles, destinées exclusivement à un cercle restreint de personnes. Dossiers du personnel, procès-verbaux de la direction, procès-verbaux du conseil d'administration.
6	Données internes	Données accessibles à l'ensemble des collaborateurs d'Agrisano. Ces données ne sont généralement ni confidentielles ni secrètes, mais elles peuvent néanmoins relever du secret d'affaires. Les échanges de courriels entre collaborateurs ainsi que les échanges non cryptés avec des tiers peuvent également être considérés comme des données internes.

7	Données publiques	Toutes les données commerciales et personnelles visibles sur le site Internet d'Agrisano, ainsi que le matériel publicitaire et les cartes de visite fournis. Par définition, les données personnelles sensibles ne sont jamais publiques.

6.8. Transmission des données

Transmission externe de données personnelles et entraide administrative (assurances sociales)

La transmission externe de données personnelles n'a lieu qu'à l'attention de personnes habilitées à cette fin. Dans le cadre de l'assurance obligatoire des soins et des assurances complémentaires, les renseignements de nature médicale ne doivent être fournis qu'après consultation du Service médecin-conseil (SMC).

Les bases suivantes sont notamment déterminantes pour la transmission externe de données personnelles :

- art. 84a LAMal et art. 97 OAMal (communication des données) ;
- art. 120 OAMal (devoir d'information des assureurs) ;
- art. 32 LPGA, art. 82 LAMal et art. 98 LAA (aide administrative) ;
- art. 47 LPGA et art. 85b LPP (consultation des dossiers) ;
- art. 86a LPP (communication des données) ;
- loi sur la protection des données (LPD) ;
- le cas échéant, une procuration de la preneuse ou du preneur d'assurance.

6.9. Profilage et décisions individuelles automatisées

La nouvelle loi sur la protection des données réglemente également le profilage, c'est-à-dire le traitement automatisé de données visant à évaluer certains aspects personnels d'une personne tels que sa situation économique, sa santé, ses intérêts, son comportement, son lieu de résidence, etc.

Si des traitements conduisent à des décisions individuelles automatisées (décisions discrétionnaires, comme le refus automatique de contrats d'assurance sur la base d'un algorithme), les responsables doivent, selon l'art. 21 LPD, assumer de nouvelles obligations d'information envers la personne lésée et lui accorder les droits d'audition et de vérification qui lui reviennent.

Les entreprises Agrisano ne pratiquent pas le profilage, ne procèdent pas à des décisions individuelles automatisées et ne prévoient pas de le faire.

6.10. Transfert de données à l'étranger

Les données personnelles ne peuvent être communiquées à l'étranger que si l'État concerné garantit une protection adéquate des données. Il existe néanmoins des exceptions à cette règle.

Agrisano ne transfère des données à l'étranger que dans des cas isolés, tout en respectant les principes de l'art. 16 et les exceptions stipulées à l'art. 17 LPD.

6.11. Réseaux sociaux

Agrisano peut être présente sur les réseaux sociaux (actuellement, il s'agit uniquement de LinkedIn, utilisé en relation avec le recrutement de personnel).

6.12. Archivage et destruction

Les documents à conserver sont archivés ou enregistrés au moins pendant la durée exigée par la loi (principalement à des fins de documentation et de preuve).

Le déroulement de la conservation, de l'archivage et de la destruction est réglé séparément.

6.13. Service de réception des données (SRD) dans le domaine du traitement électronique

Le traitement de données s'effectue sur la base de l'art. 42 LAMal, en relation avec l'art. 84 LAMal. Le traitement des données relatives au diagnostic s'effectue uniquement dans le but de contrôler les factures, compte tenu de l'obligation imposée, par les art. 42 et 56 LAMal, à l'assureur-maladie de contrôler le calcul de la rémunération et le caractère économique de la prestation.

Les dispositions d'exécution visées à l'art. 59 OAMal sont en outre prises en compte pour la facturation dans le cas d'un modèle de rémunération de type DRG (prestations stationnaires).

Le traitement électronique de type DRG est effectué par la société certifiée SRD (conformément au règlement de traitement SRD de la caisse d'assurance maladie Agrisano AG).

Un membre de la direction autorise le processus de transmission. Cette autorisation est consignée par écrit.

Le contrôle manuel des factures DRG écartées (niveau de contrôle 2) est effectué par les propres services d'Agrisano. Le processus correspondant est décrit séparément.

7. Droit d'accès, de rectification et de remise

7.1. Droit d'accès

Droit d'accès (art. 25 LPD)

Toute personne peut demander à la ou au responsable du traitement si des données personnelles la concernant sont traitées. Il s'agit des données suivantes :

a. l'identité et les coordonnées de la ou du responsable du traitement ;
b. les données personnelles traitées en tant que telles ;
c. la finalité du traitement.

En règle générale, les renseignements sont fournis dans un délai de 30 jours (pour autant que le droit en vigueur ne permette pas à Agrisano de les refuser, de les limiter ou de les différer).

Demandes de renseignements sur la santé

Lorsque les données sur l'état de santé de la requérante ou du requérant présentent un certain degré de complexité, elles sont envoyées à une ou un médecin désigné(e) par la requérante ou le requérant et non pas à la requérante elle-même ou au requérant lui-même.

7.2. Remise des données et consultation des dossiers

Droit à la remise ou à la transmission des données personnelles (art. 28 LPD)

La personne concernée peut demander à la ou au responsable du traitement qu'elle ou il lui remette sous un format électronique les données personnelles la concernant qu'elle lui a communiquées.

Consultation des dossiers selon le droit des assurances sociales

Les demandes de consultation de dossiers de la personne assurée selon l'art. 47 LPGA ou l'art. 85b LPP doivent être adressées au domaine de prestations compétent.

7.3. Rectification des données personnelles / interdiction de communiquer et de traiter des données

Une personne concernée peut interdire un certain traitement de données, demander la rectification de données personnelles inexactes ainsi que la suppression ou destruction de données ou encore en interdire la communication à des tiers.

8. Gestion de la qualité et système de contrôle interne

Le respect de la protection des données est surveillé en permanence et les mesures nécessaires sont prises en cas de non-respect. Dans le cadre du système de contrôle interne (SCI), le respect des directives de protection des données fait également l'objet d'une vérification.

En outre, pour la Caisse-maladie Agrisano SA, une certification du service de réception des données pour la facturation selon le modèle de rémunération de type DRG a lieu chaque année conformément à l'art. 59a OAMal (base légale :OCPD :2023, ordonnance sur les certifications en matière de protection des données).

9. Publication, entrée en vigueur, application et modifications

Le présent document a été élaboré en vue de l'entrée en vigueur de la loi révisée sur la protection des données au 1er septembre 2023 et remplace toutes les versions précédentes du règlement de traitement concernant le traitement des données personnelles et ses annexes. Il a été approuvé le 15 août 2023 par les directions des différentes entreprises Agrisano et entre en vigueur au 1er septembre 2023.

La directive est régulièrement actualisée et peut être modifiée à tout moment. La version publiée sur le site agrisano.ch est la version la plus récente.

Suivi des modifications :

Version	Organe de révision	Date	Remarques
1	Peter Kopp, secrétaire général	01.09.2023	Entrée en vigueur
2	Peter Kopp secrétaire général	18.08.2025	Modification rédactionnelle du ch. 1.2, modification dans la section « Conseiller/ère en protection des données » concernant la responsabilité : cette modification a été apportée lors de l'audit SRD.
3	Peter Kopp secrétaire général	26.02.2026	Modification administrative : • Suppression du ch. 2.4 « Politique de protection des données et charte de protection des données » Ce passage a été extrait des présentes directives et intégralement transféré dans le document distinct intitulé « Politique de protection des données ». • Mise à jour du ch. 8 Nouveau : VDSZ 2023 Modification rédactionnelle du ch. 6.7, des catégories de données. Modification rédactionnelle du ch. 6.13, les services de réception des données (SRD), règlement.
4	Peter Kopp secrétaire général	05.06.2026	Modification rédactionnelle par suite d'une remarque formulée lors de l'audit sur place : • Ajout du chapitre 1.6 concernant les principes du traitement des données.
5	Peter Kopp secrétaire général	06.10.2026	Complément apporté aux catégories de données du point 6.7 à la suite d'un écart mineur constaté lors de l'audit sur place.

10. Abréviations utilisées dans le présent document

Terme	Explication
CPD	Conseillère/conseiller à la protection des données
DRG	Diagnosis Related Groups (groupes de cas liés au diagnostic médical)
LAA	Loi fédérale sur l'assurance accidents
LAMal	Loi fédérale sur l'assurance-maladie
LCA	Loi fédérale sur le contrat d'assurance (loi sur le contrat d'assurance)
LPD	Loi fédérale sur la protection des données (loi sur la protection des données)
LPGA	Loi fédérale sur la partie générale du droit des assurances sociales
LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité
OAMal	Ordonnance sur l'assurance-maladie
OPDo	Ordonnance sur la protection des données
PFPDT	Préposé fédéral à la protection des données et à la transparence
SMC	Service médecin-conseil