Agrisano Stiftung
Agrisano Krankenkasse AG
Agrisano Versicherungen AG
Agrisano Pencas
Agrisano Prevos

Datenschutz-Richtlinien

Agrisano Stiftung
Agrisano Krankenkasse AG
Agrisano Versicherungen AG
Agrisano Pencas
Agrisano Prevos

Laurstrasse 10 | 5201 Brugg | Telefon +41 (0)56 461 71 11 | Fax +41 (0)56 461 71 07
info@agrisano.ch | www.agrisano.ch

Inhaltsverzeichnis

1. Allgemeine Bestimmungen

1.1. Rechtliche Grundlagen und Geltungsbereich

Grundlage für diese Datenschutzrichtlinien ist das totalrevidierte Datenschutzgesetz (DSG), die Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV) und die neue Verordnung über Datenschutzzertifizierungen (VDSZ), mit Inkrafttreten per 1. September 2023.

Das revidierte Datenschutzgesetz beschränkt sich auf den Datenschutz natürlicher Personen – statt wie bisher auch auf Daten juristischer Personen. Das Gesetz gilt für die Bearbeitung von Personendaten durch «private Personen» und «Bundeorgane».

Krankenkassen gelten im Bereich des Krankenversicherungsgesetzes (KVG) als Bundesorgane und im Bereich des Versicherungsvertragsgesetzes (VVG) als private Bearbeiter. Die Agrisano Krankenkasse AG betreibt die obligatorische Krankenpflegeversicherung (OKP) und gilt somit als Bundesorgan.

Pensionskassen bzw. Vorsorgestiftungen gelten als Bundesorgane, wenn sie (ganz oder teilweise) im obligatorischen Bereich tätig sind. Agrisano Pencas gilt somit aufgrund des obligatorischen Teils als Bundesorgan. Agrisano Prevos zählt zusammen mit der Agrisano Stiftung und der Agrisano Versicherungen AG zu den privaten Personen. Spezifische Datenschutznormen (z.B. Art. 86a BVG) gehen jenen des DSG vor.

Die Prozesse zur Bearbeitung von Daten sind in allen Agrisano-Unternehmungen identisch.

1.2. Verantwortlichkeiten innerhalb der Agrisano-Unternehmungen

Die Gesamtverantwortung für den Datenschutz trägt das Leitungsorgan der jeweiligen Agrisano-Unternehmung. Diese Verantwortung ist nicht übertragbar.

Für die Umsetzung des Datenschutzes im Betrieb ist der/die Datenschutzberater/in verantwortlich. Der/die Datenschutzberater/in kontrolliert die Einhaltung des Datenschutzes, berät die Geschäftsleitung und die Mitarbeitenden und unterstützt sie bei der operativen Umsetzung des Datenschutzes im Betrieb.

Agrisano betreibt die Informatik-Systeme mit einem eigenen, internen Informatik-Team. Das Team IT-Operations besteht aus sechs Mitarbeitenden (mit speziellen Zugriffs- und Zutrittsberechtigungen) und ist für den gesamten Betrieb und die Infrastruktur zuständig.

1.3. Geheimhaltung und Schweigepflicht

Mitarbeitende

Für die Erfüllung ihrer Aufgaben bearbeiten die Mitarbeitenden der Agrisano Personendaten, auch besonders schützenswerte, in den Informatiksystemen.

Agrisano misst dem Datenschutz einen hohen Stellenwert zu, hält sich an die Datenschutzgesetzgebung und regelt den Datenschutz in verschiedenen, allen Mitarbeitenden zugänglichen Dokumenten. Sämtliche Mitarbeitenden unterstehen der beruflichen Schweigepflicht gemäss Art. 62 DSG und verpflichten sich mit der Unterzeichnung des Arbeitsvertrages zu Verschwiegenheit, Geheimhaltung und zur Einhaltung der Datenschutzgesetzgebung.

Externe Partner

Mit den externen Partnern der Agrisano-Unternehmungen bestehen Zusammenarbeitsverträge. Die Partner verpflichten sich vertraglich, die Datenschutzbestimmungen im gleichen Umfang wie die Agrisano einzuhalten.

1.4. Datenschutzberater/in und Kontaktstelle für datenschutzrechtliche Fragen

Private Unternehmen (also die Agrisano Stiftung, die Agrisano Versicherungen AG und die Agrisano Prevos) können eine Datenschutzberaterin oder einen Datenschutzberater (DSB) ernennen; Bundesorgane (die Agrisano Krankenkasse AG und die Agrisano Pencas) haben hingegen die gesetzliche Pflicht dazu. Hier sind die Datenschutzberatenden nicht nur eine innerbetriebliche Anlaufstelle, sondern auch Bindeglied zum behördlichen Datenschutz und erste Ansprechpersonen für den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Für sämtliche Fragen und Anliegen in Zusammenhang mit dem Datenschutz (insbesondere auch die Abwicklung von Auskunftsgesuchen seitens Dritter, Prüfen der Bekanntgabe von Personendaten an Dritte, Bearbeitung und Prüfung von Datenschutzverletzungen) kann bei allen Agrisano-Unternehmungen folgende Stelle kontaktiert werden:

Agrisano
Datenschutzberater/in
Laurstrasse 10
5201 Brugg
Tel. +41 56 461 71 11 / Mail: datenschutz@agrisano.ch

Datenschutz-Anliegen sind schriftlich und unter Beilage einer Ausweiskopie (um die Identität zu prüfen und Missbrauch auszuschliessen) an obige Adresse zu richten.

1.5. Personendaten

Das revidierte DSG bezweckt ausschliesslich den Schutz der Persönlichkeit von **natürlichen** Personen, über welche Personendaten bearbeitet werden. Daten von juristischen Personen wie kaufmännische Gesellschaften, Vereine oder Stiftungen werden vom neuen DSG nicht mehr erfasst.

Als Personendaten oder auch personenbezogene Daten gelten alle Daten, die sich auf eine Person beziehen und diese identifizieren oder zur Identifizierung der Person beitragen. Das Datenschutzgesetz unterscheidet dabei zwischen **Personendaten** und **besonders schützenswerten Personendaten**. Schützenswert sind dabei grundsätzlich alle Personendaten. Im Zusammenhang mit der Bearbeitung von besonders schützenswerten Personendaten sieht das Gesetz jedoch zusätzliche Anforderungen vor.

Als **besonders schützenswerte Personendaten** gelten gemäss DSG:

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
- Daten über die Gesundheit*, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
- genetische Daten,
- biometrische Daten, die eine natürliche Person eindeutig identifizieren,
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
- Daten über Massnahmen der sozialen Hilfe.

* Insbesondere folgende Daten können Informationen über die Gesundheit einer Person enthalten: Aufzeichnung über den Verlauf einer Behandlung, Beschreibung von Symptomen, Diagnosen, ärztliche Verordnungen / Berichte / Spitalberichte, Therapien, Medikamente, Überweisungen, Laborresultate, Tarifpositionen, Aufzeichnungen von bildgebenden Verfahren.

2. Organisation und Datenschutzleitbild

2.1. Geschäftsstelle der Agrisano

Die fünf Agrisano-Unternehmungen beschäftigen insgesamt ca. 220 Mitarbeitende (Stand: April 2023 / über keine eigenen Mitarbeitenden verfügt die Agrisano Versicherungen AG).

2.2. Regionalstellen der Agrisano

Die Agrisano arbeitet eng mit den kantonalen landwirtschaftlichen Berufsorganisationen zusammen, welche für die Agrisano regionale Geschäftsstellen (Regionalstellen) betreiben.

Die Regionalstellen verfügen über eine eigene Informatik-Infrastruktur und greifen über eine gesicherte Verbindung zu Agrisano ausschliesslich auf benötigte Systeme und Programme zu.

2.3. Organigramme

Die aktuellen Organigramme finden sich auf der Website unter «Auf einen Blick» (Unternehmungen - Agrisano - Schweizer Bauernverband).

2.4. Datenschutzpolitik bzw. Datenschutzleitbild

Die Agrisano-Unternehmungen verpflichten sich zur Einhaltung der geltenden Datenschutzvorschriften sowie der speziellen branchenspezifischen Vorschriften und setzen sich für eine kontinuierliche Verbesserung der Wirksamkeit des Datenschutzes ein.

Zweckmässigkeit

Die Agrisano-Unternehmungen bearbeiten Personendaten ausschliesslich zum Zweck der ihr gesetzlich übertragenen Aufgaben oder im Rahmen der Zustimmung der betroffenen Personen. Es werden nur diejenigen Personendaten erfasst, welche für die Geschäftstätigkeit notwendig sind.

Verhältnismässigkeit

Es werden nur so viele Personendaten bearbeitet, wie zwingend notwendig, um den Zweck zu erreichen. Zugriffsrechte werden restriktiv vergeben. Jeder Mitarbeiter resp. jede Mitarbeiterin kann nur auf diejenigen Daten zugreifen, die für die Erfüllung der Aufgaben notwendig sind.

Aufbewahrung und Archivierung

Die Agrisano-Unternehmungen verwahren Personendaten grundsätzlich so lange, wie sie gesetzlich dazu verpflichtet sind. Unterliegen die Daten keinen Aufbewahrungsvorschriften, werden sie nur so lange aufbewahrt, wie sie für die Zweckerreichung von Bedeutung sind.

Datensicherheit

Es werden alle geeigneten technischen und organisatorischen Sicherheitsmassnahmen getroffen, um die verwalteten Personendaten vor unberechtigtem oder unrechtsmässigem Zugriff, Verlust, Vernichtung oder Beschädigung zu schützen.

3. Datenzugriffe und Benutzer

3.1. Grundsatz

Benutzerinnen und Benutzer erhalten nur auf diejenigen Daten, Programme und Funktionen Zugriff, die sie zum Ausüben ihrer Tätigkeit benötigen (ihren Aufgaben entsprechend werden sie in Gruppen zusammengefasst). Die Zugriffsrechte der Gruppen sind auf die Funktion und Tätigkeitsfelder zugeschnitten (inkl. der Unterscheidung zwischen Lese- oder Änderungsberechtigung).

Für den allgemeinen Umgang bezüglich Nutzung der IT-Anlage gibt es separate Weisungen.

3.2. Benutzerrechte und Benutzerverwaltung

Die Vergabe von Zugriffsrechten ist an die jeweilige Funktion gebunden und in einem Berechtigungskonzept geregelt. Zusätzliche Berechtigungen einer Funktion, die vom Berechtigungskonzept abweichen, können nur durch den jeweiligen Daten-Owner beantragt werden. Sämtliche Berechtigungen (inkl. privilegierten Benutzerrechten) werden einer jährlichen Kontrolle durch die Daten-Owner unterzogen.

3.3. Persönliche Zugriffsberechtigung / Benutzer-Authentisierung

Die Informatik-Systeme der Agrisano dürfen nur mit dem persönlichen Benutzernamen und dem entsprechenden Passwort (die Passwortkomplexität ist separat geregelt) benutzt werden. Die Weitergabe des persönlichen Passworts ist untersagt. Die Komplexität des Passworts wird zudem systemtechnisch geprüft und auch der Passwortwechsel wird aufgrund eines zeitlichen Limits verlangt.

Der Zugriff auf die Agrisano-Informatikinfrastruktur ist von extern ausschliesslich über einen IPSec-Tunnel oder VPN-Client mit Zwei-Faktor-Authentisierung (z.B. aus dem Homeoffice) möglich.

3.4. Aufhebung Zugriffsberechtigung

Die Zugriffsberechtigungen zur IT der Agrisano gelten nur für die Dauer der Arbeitsfunktion. Bei Austritt werden die Zugriffsberechtigungen entzogen, bei Aufgabenwechsel innerhalb Agrisano werden die Zugriffsberechtigungen für den neuen Aufgabenbereich zugewiesen.

4. Weitere Pflichten des Verantwortlichen (Agrisano)

4.1. Anmeldung der Datensammlungen bzw. Meldung der Bearbeitungsverzeichnisse beim EDÖB

Mit der Inkraftsetzung des neuen Datenschutzgesetzes (DSG) erfährt die Anmeldung von Datensammlungen im Register des EDÖB eine Änderung. Ab diesem Zeitpunkt müssen nur noch Bundesorgane (also die Agrisano Krankenkasse AG sowie die Agrisano Pencas) ihre Datensammlungen (neu: Einträge aus dem Verzeichnis der Bearbeitungstätigkeiten gemäss Artikel 12 DSG) dem EDÖB melden. Private (Agrisano Stiftung, Agrisano Versicherungen AG sowie Agrisano Prevos) werden von der Meldepflicht befreit.

Der EDÖB veröffentlicht die Meldungen der Bundesorgane in einem öffentlich zugänglichen Register, dem DataReg. Für die Pflege des Registers ist der/die Datenschutzberater/in zuständig.

4.2. Meldung von Datenschutzverletzungen an den EDÖB

Verletzungen von Datensicherheit, das heisst unbeabsichtigtes oder widerrechtliches Verlieren, Löschen, Vernichten, Verändern oder Unbefugten zugänglich machen von Personendaten, müssen dem EDÖB so rasch als möglich gemeldet werden, wenn sie voraussichtlich zu einem hohen Risiko für die Betroffenen führen (Verletzung der Datensicherheit).

Auf der Website des EDÖB gibt es hierfür ein spezielles Meldeportal (EDOEB DataBreach (admin.ch)).

In der Regel muss der Verantwortliche auch die betroffene/n Person/en informieren, wenn dies zu ihrem Schutz nötig ist oder der EDÖB es verlangt.

Das Vorgehen und der Meldeprozess sind separat geregelt und gelten für alle Agrisano-Unternehmungen sowie die Regionalstellen.

5. Technische und organisatorische Massnahmen zur Gewährleistung der Datensicherheit

5.1. Grundsätze

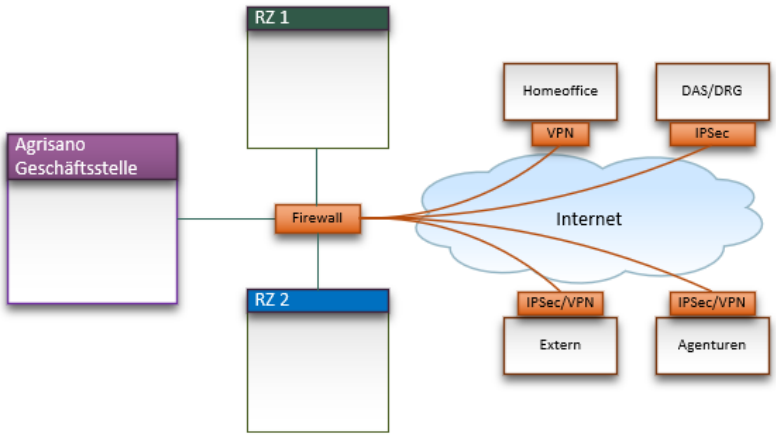
Zur Gewährleistung einer angemessenen Datensicherheit werden verschiedene technische und organisatorische Massnahmen getroffen. Es wird den folgenden Zielen gemäss Datenschutzverordnung Rechnung getragen, wonach die Daten:

- nur Berechtigten zugänglich sind (Vertraulichkeit);
- verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
- nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
- nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

5.2. IT-Struktur

Agrisano verfügt über zwei dezentrale Rechenzentren, welche über verschiedene technische Einrichtungen (z.B. unterbrechungsfreie Stromversorgung, Klimaanlage, Brandmeldesystem, Alarmierung etc.) besonders geschützt und ausschliesslich für den Zugang durch speziell berechtigte Personen gesichert sind. Die durch die Agrisano-IT betriebenen Server sind ebenfalls den hohen Sicherheitsanforderungen entsprechend ausgestattet.

Die grafische Darstellung zeigt die Informatik-Struktur inkl. Anbindung der Stellen und Benutzer ausserhalb über IPSec/VPN-Tunnel:



5.3. Zugangskontrolle (Gebäudezutritt)

Am Agrisano-Hauptsitz sind sämtliche Räumlichkeiten, in welchen Personendaten bearbeitet werden, elektronisch und mechanisch vor dem Zutritt unbefugter Personen gesichert. Das elektronische Schliesssystem am Hauptsitz (mit persönlichem Schlüssel, «Badge» genannt) basiert auf einer eigenen Benutzerverwaltung. Diese Badges sind persönlich und dürfen anderen Mitarbeitenden bzw. Drittpersonen nicht überlassen werden.

Besonders sensitive Räume, z.B. jene der Gruppe Stationär (DAS) oder der VAD-Bereich sind räumlich getrennt. Die Technikräume und die Rechenzentren sind zusätzlich speziell gesichert (inkl. eingeschränktem Zutritt und separaten Sicherheitssystemen). Auch die Zutrittsberechtigung zum Archiv wird restriktiv gehandhabt.

5.4. Authentifizierung

Durch verschiedene Massnahmen (z.B. mittels Einhaltung Berechtigungskonzept, Verwaltung/Vergabe der Berechtigung durch Systemadministratoren, Passwortrichtlinie etc.) wird gewährleistet, dass Berechtigte ausschliesslich auf die aufgrund ihrer Zugriffsberechtigung freigegeben Daten zugreifen können. Weitere Regelungen zur Authentifizierung siehe Ziff. 3.

5.5. Kontrollen und Protokollierung

Kontrollen

- **Bekanntgabekontrolle**
  Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden über die Schnittstellen bzw. gesicherte Leitungen identifiziert.
- **Speicherkontrolle**
  Die einzelnen Benutzer erhalten spezifische Berechtigungen für Mutationen in Datenfeldern, die sie für die Erfüllung ihrer Aufgaben (z.B. gemäss KVG) benötigen.

Protokollierung

Zugriffe auf die IT-Systeme der Agrisano werden über das Benutzer-Berechtigungskonzept möglichst eingeschränkt (so erfordert z.B. das Löschen von Personendaten die höchste Berechtigungsstufe). Da die Nutzung der Applikationen immer über die persönliche User-ID und Autorisierung erfolgt, wird damit auch das Bearbeiten von Personendaten historisiert (Protokolle für sämtliche vorgenommenen Änderungen werden nicht erstellt, auf Anfrage erfolgt eine individuelle Abfrage in der Datenbank).

Zugriffe externer Dienstleister oder Auftragsbearbeiter werden gesichert und historisiert, zudem verfügen diese über eigene interne Regelungen zur Protokollierung.

5.6. Weitere technische Massnahmen zum Schutz der Daten

Nachfolgend die wichtigsten technischen Massnahmen:

- **Daten-Übermittlung** (z.B. E-Mails) via Verschlüsselungsverfahren;
- **Technische Anforderungen an Endgeräte**: Zugangsbeschränkung zum internen Netzwerk von Agrisano, der externe Zugriff erfolgt über VPN;
- **Datensicherung:** Backups sowie Spiegelung der Speichersysteme an verschiedenen Standorten;
- **IT-Sicherheit:** Firewall, Endpoint-Schutz und Spamfilter;
- **Systemsicherheit:** Betriebssysteme und Anwendungssoftware wird stets auf dem neusten Sicherheitsstand gehalten und bekannte Lücken werden zeitnah geschlossen.

5.7. Organisatorische Massnahmen zum Schutz der Daten

Die Agrisano-Mitarbeitenden sind angewiesen, den Bildschirm beim Verlassen des Arbeitsplatzes zu sperren (dies gilt auch im Homeoffice).

Ausgedruckte Daten werden so aufbewahrt, dass Drittpersonen (z.B. Raumpflegepersonal) diese nicht einsehen und/oder kopieren können.

Für den Umgang mit besonders schützenswerte Personendaten gibt es verschiedene interne Weisungen, z.B. bezüglich Aufbewahrung in abschliessbaren Behältnissen, Aktenvernichtung via Entsorgungssystem «DATAEX 4000 AG» etc.

Bei Agrisano gilt grundsätzlich das Clean-Desk- sowie das Clear-Screen-Prinzip.

5.8. Privacy-by-Design und Privacy-by-Default

«Privacy-by-Design and Privacy-by-Default» sind explizit unter «Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen» (Art. 7 DSG) verankert.

Bei der Verarbeitung von Personendaten müssen «schon bei der Planung» angemessene technische und organisatorische Massnahmen (TOM) getroffen werden, welche die Umsetzung von Datenschutzgrundsätzen (z.B. Datenminimierung) in diesen Systemen sicherstellen (Privacy-by-Design). Auch die Voreinstellungen, beispielsweise bei Apps oder Websites, sind so auszugestalten, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck «nötige Mindestmass beschränkt ist» (Privacy-by-Default).

6. Datenbearbeitung

6.1. Bearbeitung durch Auftragsbearbeiter

Gemäss Art. 9 DSG kann die Bearbeitung von Personendaten vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, sofern die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

Die Agrisano-Unternehmungen arbeiten konzern-intern und mit Dritten zusammen.

6.2. Zweck der Datenbearbeitung

Agrisano bearbeitet Daten ausschliesslich zum Zweck der Durchführung des von ihr betriebenen Versicherungsgeschäfts und angebotenen Vorsorgelösungen, insbesondere zur Dokumentation der Versicherungs- und Vorsorgeverhältnisse, der Antragsprüfung, der Leistungsverarbeitung, der Limitationsprüfung, der Zahlungsverarbeitung sowie zur Führung von Statistiken und zur Auskunftserteilung. Die Daten werden somit ausschliesslich in Erfüllung der gesetzlichen Rechte und Pflichten bearbeitet.

Zusätzlich werden im Rahmen der allgemeinen Geschäftstätigkeit Daten von Leistungserbringern, Dienstleistern, Lieferanten, Partner-Firmen, Banken, Behörden und Ämtern, etc. bearbeitet. Hier handelt es sich in der Regel jedoch um Daten juristischer Personen, welche nicht mehr explizit unter das Datenschutzgesetz fallen.

6.3. Art der Daten

Kunden-/Personendaten: Stamm- und Bestandesdaten (z.B. Vorname/Name, Adresse, Nationalität, Geburtsdatum, Zivilstand, AHV- und Versichertennummer, Sprachen, Nationalität, Kantons- und Gemeindezugehörigkeit, Telefonnummer, E-Mail-Adresse, Familienangehörige, Bevollmächtige, Bankverbindung und Zahlungsinformationen).

Kommunikationsdaten: Sämtliche Daten betr. persönlicher, telefonischer und schriftlicher Kommunikation (Post und E-Mails), Kontaktanfragen über Website, Umfragedaten, Newsletter, etc.

Antragsdaten: Daten in Zusammenhang mit Offertanfragen oder Beitrittsanträgen (z.B. Personalien, gewünschte Versicherungsmodelle, Gesundheitsdeklarationen).

Vorsorge-/Versicherungsvertrags- und Prämiendaten (Individual- und Kollektivverträge): Art der Versicherung, Abschluss, Laufzeit, Prämien, Franchisen, Versicherungssummen, etc.

Leistungsdaten (inkl. Case Management): Daten der Leistungserbringer, wie z.B. Rechnungen/Kosten, Diagnosen, Arztberichte, etc.

VAD-Daten: Unterlagen des vertrauensärztlichen Dienstes, z.B. Leistungsansprüche, Diagnosen, medizinische Gutachten.

Auszahlungs- und Inkassodaten: Daten in Zusammenhang mit dem Rechnungswesen, wie z.B. offene Posten, Zahlungen und Fakturierungen, Rückforderungen.

Marketingdaten: Kundenmagazin, Daten Marketingaktionen, Ergebnisse aus Kundenumfragen, Wettbewerbsteilnahmen (z.B. Kontaktdaten, Präferenzen, Bedürfnisse).

HR-Daten: Personenstammdaten und Daten aus dem Personaldossier (z.B. Bewerbungsunterlagen, Mitarbeiterbeurteilungen, Zeugnisse, Aus- und Weiterbildungen, Arbeitszeiten, Lohnbearbeitungsdaten).

Compliance-Daten und Datenschutz-Daten: Daten in Zusammenhang mit Compliance-Beurteilungen oder Datenschutzverletzungen (Angaben über betroffene und involvierte Personen).

Userdaten, Systemnutzungsdaten und technische Daten: Daten in Zusammenhang mit der Benutzerverwaltung (z.B. Personalien, Funktion, Zugangsdaten), Nutzung der IT-Systeme oder der Website von Agrisano (z.B. Geschäftsnummern, IP-Adressen, interne und externe Kennungen, Aufzeichnungen von Zugriffen).

Daten der Videoüberwachungskamera: Bilddateien der Überwachungskameras im Aussenbereich und in der Autoeinstellhalle des Agrisano-Hauptsitzes in Windisch.

6.4. Verzeichnis der Bearbeitungstätigkeiten

Gemäss Art. 12 DSG ist ein Verzeichnis der Bearbeitungstätigkeiten zu führen; die nötigen Angaben sind im DSG vorgeschrieben. Dieses Verzeichnis wurde durch die Agrisano-Unternehmungen im 2023 neu erstellt. Es wird laufend ergänzt und periodisch überprüft und aktualisiert.

Während Bundesorgane (also die Agrisano Krankenkasse AG sowie die Agrisano Pencas) dem EDÖB die Verzeichnisse melden müssen, sieht das neue Recht für die privaten Datenbearbeiter keine Meldepflicht mehr vor.

6.5. Dokumentation von Datensammlungen

Die Datensammlungen mit besonders schützenswerten Personendaten der Agrisano-Unternehmungen werden in einzelnen verschiedenen Reglementen, Weisungen und Richtlinien dokumentiert. Für Abläufe, bei denen besonders schützenswerte Personendaten bearbeitet werden (u.a. DRG-Datenannahmestelle) bestehen ausführliche Dokumentationen.

6.6. Datenherkunft

Überlassene Daten

Personendaten werden Agrisano häufig selbst bekanntgegeben (z.B. über Formulare, bei der Kommunikation mit Agrisano, bei Verwendung der Website etc.). Werden Verträge mit Agrisano abgeschlossen oder Leistungen beansprucht, werden Agrisano verschiedene Daten überlassen (z.B. Personenstamm-, Antrags- oder Vertragsdaten).

Erhaltene Daten

Personendaten werden Agrisano teilweise auch von Dritten übermittelt, dies können sein:

- öffentliche Ämter und Register (z.B. Einwohnerkontrolle, Betreibungsregister etc.) oder die schweizerische Post;
- Behörden, Gerichte, Parteien und andere Dritte im Zusammenhang mit behördlichen und gerichtlichen Verfahren;
- Arbeitgebende;
- Personen aus dem Umfeld (Familie, Berater, Rechtsvertreter etc.), Bevollmächtigte;
- Banken und anderen Finanzdienstleistern, Privat- und Sozialversicherungen, Vorsorge- und Freizügigkeitseinrichtungen;

- Spitäler, Ärzte und andere Leistungserbringer, Sachverständige, Gutachtende;
- Dienstleistende (z.B. den Agenturen);
- Personalvermittelnde (z.B. Stellenvermittler, Headhunter).

6.7. Datenkategorien

Bei der Bearbeitung der Daten wird der definierten Datenkategorie Rechnung getragen. Folgende Datenkategorien wurden in Zusammenhang mit dem Datenschutz definiert:

1	Besonders schützenswerte Personendaten	Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, über Massnahmen der sozialen Hilfe; verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen und auch genetische und biometrische Daten. Bei Bearbeitung dieser Daten ist äusserste Sorgfalt walten zu lassen.
2	Personendaten mit geringer Datenschutzrelevanz	Daten, welche gemäss DSG nicht als «besonders schützenswert» gelten, jedoch eher sensitiv oder vertraulich sind und mit grösserer Sorgfalt behandelt werden.
3	Personendaten ohne datenschutzrechtliche Relevanz	Daten, die eine natürliche Person nicht eindeutig identifizieren, also Informationen, die einzig Name, Vorname und Adresse oder eine interne Anschrift enthalten. Mit den Daten wird sorgfältig umgegangen.

6.8. Datenweitergabe

Externe Weitergabe von Personendaten und Verwaltungshilfe (Sozialversicherungen)

Eine externe Weitergabe von Personendaten erfolgt nur an Berechtigte. Auskünfte medizinischer Art sind im Falle der obligatorischen Krankenpflegeversicherung und den Krankenzusatzversicherungen nur nach Rücksprache mit dem Vertrauensärztlichen Dienst (VAD) zu gewähren.

Massgebend für die externe Weitergabe von Personendaten sind insbesondere folgende Grundlagen:

- Art. 84a KVG und Art. 97 UVG (Datenbekanntgabe);
- Art. 120 KVV (Informationspflicht der Versicherer);
- Art. 32 ATSG, Art. 82 KVG und Art. 98 UVG (Verwaltungshilfe);
- Art. 47 ATSG und Art. 85b BVG (Akteneinsicht);
- Art. 86a BVG (Datenbekanntgabe)
- Datenschutzgesetz (DSG);
- Gegebenenfalls Vollmacht des Versicherungsnehmers.

6.9. Profiling und automatisierte Einzelentscheidungen

Das neue Datenschutzgesetz regelt auch das Profiling, das heisst die automatisierte Datenbearbeitung, um bestimmte persönliche Aspekte einer Person wie wirtschaftliche Lage, Gesundheit, Interessen, Verhalten, Aufenthaltsort usw. zu bewerten.

Führen Bearbeitungen zu automatisierten Einzelentscheidungen (Ermessensentscheide, wie z.B. automatische Ablehnung von Versicherungsverträgen aufgrund eines Algorithmus), haben die Verantwortlichen nach Art. 21 DSG neue Informationspflichten gegenüber der beschwerten Person wahrzunehmen und dieser die ihr zustehenden Anhörungs- und Überprüfungsrechte zu gewähren.

Die Agrisano-Unternehmungen betreiben kein Profiling, führen keine automatisierten Einzelentscheidungen durch und haben dies auch nicht geplant.

6.10. Datentransfer ins Ausland

Personendaten dürfen nur dann ins Ausland bekannt gegeben werden, wenn der betreffende Staat einen angemessenen Datenschutz gewährleistet. Zu dieser Vorgabe gibt es Ausnahmen.

Datentransfers ins Ausland finden bei Agrisano nur in Einzelfällen statt, dabei werden die Grundsätze gemäss Art. 16 und Ausnahmen gemäss Art. 17 DSG eingehalten.

6.11. Soziale Netzwerke (Social Media)

Agrisano kann auf sozialen Netzwerken präsent sein (aktuell ist dies lediglich die Seite auf LinkedIn, welche in Zusammenhang mit Personalrekrutierung genutzt wird).

6.12. Archivierung und Vernichtung

Aufbewahrungspflichtige Dokumente werden mindestens während der gesetzlich verlangten Dauer archiviert bzw. gespeichert (primär zu Dokumentations- und Beweiszwecken).

Der Ablauf der Aufbewahrung, Archivierung und Vernichtung ist separat geregelt.

6.13. Datenannahmestelle (DAS) im Bereich der elektronischen Bearbeitung (umfassendes Outsourcing)

Die Datenbearbeitung erfolgt gestützt auf Art. 42 KVG i.V.m. Art. 84 KVG. Die Bearbeitung der Diagnosedaten erfolgt ausschliesslich zur Überprüfung der Rechnungen auf die durch Art. 42 KVG und Art. 56 KVG vorgegebene Pflicht des Krankenversicherers, die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung zu prüfen.

Im Falle der Rechnungsstellung bei einem Vergütungsmodell vom Typus DRG (stationäre Leistungen) werden zusätzlich die Ausführungsbestimmungen nach Art. 59a KVV berücksichtigt.

Die elektronische Bearbeitung vom Typus DRG (Prüfungsstufe 1) erfolgt durch die zertifizierte DAS der ÖKK-Gruppe (gemäss Bearbeitungsreglement DAS der ÖKK und Outsourcingvertrag zwischen der ÖKK und der Agrisano).

Ein Mitglied der Geschäftsleitung bewilligt den Auslenkungsprozess. Diese Bewilligung wird schriftlich festgehalten.

Die manuelle Prüfung der ausgelenkten Belege vom Typus DRG (Prüfungsstufe 2) findet bei der Agrisano durch eigene Stellen statt. Der entsprechende Prozess ist separat beschrieben.

7. Recht auf Auskunft, Berichtigung und Datenherausgabe

7.1. Auskunftsrecht

Auskunftsrecht (Art. 25 DSG)

Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Es sind dies folgende Daten:

a. die Identität und die Kontaktdaten des Verantwortlichen;
b. die bearbeiteten Personendaten als solche;
c. der Bearbeitungszweck.

Die Auskunft wird in der Regel innert 30 Tagen erteilt (sofern diese nach geltendem Recht seitens Agrisano nicht verweigert, eingeschränkt oder aufgeschoben werden darf).

Auskunftsbegehren über die Gesundheit

Daten über die Gesundheit des Gesuchstellers, die einen gewissen Komplexitätsgrad aufweisen, werden an einen vom Gesuchsteller bestimmten Arzt übermittelt und nicht an den Gesuchsteller persönlich.

7.2. Datenherausgabe und Akteneinsicht

Datenherausgabe oder -übertragung (Art. 28 DSG)

Jede Person kann vom Verantwortlichen die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in elektronischer Form verlangen.

Akteneinsicht nach Sozialversicherungsrecht

Akteneinsichtsgesuche der versicherten Person nach Art. 47 ATSG oder Art. 85b BVG sind an den zuständigen Leistungsbereich zu richten.

7.3. Berichtigung Personendaten / Verbot Bekanntgabe und Bearbeitung von Daten

Eine betroffene Person kann eine bestimmte Datenbearbeitung verbieten, die Berichtigung unrichtiger Personendaten sowie eine Datenlöschung/-vernichtung verlangen oder auch die Bekanntgabe an Dritte verbieten.

8. Qualitätsmanagement und Internes Kontrollsystem

Die Einhaltung des Datenschutzes wird laufend überwacht und bei Missachtung werden die erforderlichen Massnahmen eingeleitet. Im Rahmen des internen Kontrollsystems (IKS) wird ebenfalls überprüft, ob die Datenschutzvorgaben eingehalten werden.

Zudem findet für die Agrisano Krankenkasse AG jährlich eine Zertifizierung der Datenannahmestelle für die Rechnungsstellung nach Vergütungsmodell vom Typus DRG gemäss Art. 59a KVV statt (normative Grundlage: VDSZ:2014 Verordnung über die Datenschutz-Zertifizierungen und basierend auf einem gültigen Zertifikat der ÖKK).

9. Publikation, Inkrafttreten, Anwendung und Änderungen

Das vorliegende Dokument entstand im Hinblick auf die Inkraftsetzung des revidierten Datenschutzgesetzes per 1. September 2023 und ersetzt die alle bisherigen Versionen von «Bearbeitungsreglement betreffend den Umgang mit Personendaten und Anhänge». Es wurde am 15. August 2023 durch die Geschäftsleitungen der einzelnen Agrisano-Unternehmungen genehmigt und tritt per 1. September 2023 in Kraft.

Die Richtlinie wird regelmässig aktualisiert und kann jederzeit geändert werden. Die auf der Website agrisano.ch veröffentlichte Version ist die jeweils aktuelle Fassung.

Änderungsnachweis:

Version	Prüfstelle	Datum	Bemerkungen
1	Peter Kopp, Generalsekretär	01.09.2023	Inkraftsetzung

10. Abkürzungsverzeichnis

Begriff	Erklärung
ATSG	Bundesgesetz über Allgemeinen Teil des Sozialversicherungsrechts
BVG	Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenversicherung
DRG	Diagnosis Related Groups (Diagnosebezogene Fallgruppen)
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz)
DSV	Verordnung über den Datenschutz (Datenschutzverordnung)
DSB	Datenschutzbeauftragter
EDÖB	Eidg. Datenschutz- und Öffentlichkeitsbeauftragter
KVG	Bundesgesetz über die Krankenversicherung
KVV	Verordnung über die Krankenversicherung
UVG	Bundesgesetz über die Unfallversicherung
VAD	Vertrauensärztlicher Dienst
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VVG	Bundesgesetz über den Versicherungsvertrag (Versicherungsvertragsgesetz)