ALTERSZENTRUM
BREMGARTEN

Konzept

Datenschutz und Datensicherheit

Erlassen durch den Verwaltungsrat am	26.10.2023
Ersetzt Konzept vom	7.4.2022
Letzte Überprüfung/Anpassung am	
Nächste Überprüfung am	2025

Kalchackerstrasse 20 | 3047 Bremgarten bei Bern | www.alterszentrum3047.ch | info@alterszentrum3047.ch | T 031 300 51 10

Inhalt

1. Zweck dieses Konzepts

Der Hauptzweck des vorliegenden Datenschutzkonzepts des Alterszentrum Bremgarten (AZB) ist die Gewährleistung des Schutzes der Persönlichkeit natürlicher Personen vor widerrechtlicher oder unverhältnismässiger Bearbeitung ihrer Daten im Verantwortungsbereich des AZB. Es betrifft dies namentlich dessen Bewohnerinnen und Bewohner, dessen Kundinnen und Kunden, dessen Mitarbeitenden und dessen Geschäftspartnerinnen und –partner.

Es bildet die verbindliche Grundlage für alle in den Diensten des AZB tätigen Personen, in Eigenverantwortung bei der Durchführung aller datenschutzrelevanten Massnahmen und Aktivitäten datenschutzrechtlich einwandfrei zu handeln, namentlich beim Bearbeiten von

- Personendaten der Bewohnerinnen, Bewohner, Kundinnen und Kunden;
- Personendaten der Mitarbeitenden, inklusive Daten über Stellenbewerbende und ehemalige Mitarbeitende;
- Informationen über Geschäftspartnerinnen, -partner und weiteren Dritte, soweit Personendaten betroffen sind.

Im Weiteren werden die spezifischen datenschutzrelevanten Anforderungen für das elektronische Patientendossier (EPD) festgehalten.

2. Rechtliche Grundlagen

Grundlagen für dieses Datenschutzkonzept sind

- das Bundesgesetz über den Datenschutz vom 25. September 2020 (DSG; SR 235.1),
- die Verordnung über den Datenschutz vom 31. August.2022 (DSV; SR 235.11),
- das Datenschutzgesetz des Kantons Bern vom 19. Februar 1986 (KDSG; BSG 152.04),
- die Datenschutzverordnung des Kantons Bern vom 22. Oktober 2008 (DSV; BSG 152.040.1),
- die Verordnung über das elektronischen Patientendossier vom 22. März 2017 (EPDV; SR 816.11),
- die DSDS-Policy und Richtlinien der EPD-Stammgemeinschaft vom 14.02.2020.

3. Geltungsbereich

Das vorliegende Datenschutzkonzept gilt für alle Organe und Mitarbeitenden des AZB, die im Rahmen der Erfüllung ihrer Funktionen und Aufgaben Personendaten bearbeiten.

Es gilt ebenfalls für externe Personen und Firmen, sofern sie sich durch entsprechende schriftliche Vereinbarung zu dessen Einhaltung verpflichten.

4. Begriffe und Abkürzungen

Wichtige Begriffe und Abkürzungen sind in Anhang 1 definiert.

5. Geschützte Daten

Geschützte Daten sind alle Personendaten (Daten), d.h. alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Darunter fallen unter anderem Adressen, Telefonnummern, Altersangaben usw., die geheim zu halten und vor fremdem Zugriff zu schützen sind.

Ein Teil dieser Daten sind besonders schützenswerte Personendaten. Es sind dies Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe oder über administrative bzw. strafrechtliche Verfolgungen und Sanktionen.

Bei den im AZB erhobenen und aufbewahrten Daten von Personen handelt es sich überwiegend um besonders schützenswerte Daten. So erhöhen Angaben über Vermögensverhältnisse, Zahlungsverbindungen, Angehörigenumfeld und erst recht pflegerische und medizinische Belange (etwa Bedarfsabklärungen, Pflegeeinstufungen, medizinische Diagnosen oder Medikamentenliste) die Datensensibilität und erfordern einen besonders sorgsamen Umgang mit ihnen.

6. Grundsätze des Datenschutzes

6.1 Rechtmässigkeit

Die Datenbearbeitung ist rechtmässig, wenn sie durch die Einwilligung der betroffenen Person, ein überwiegendes öffentliches oder privates Interesse oder durch Gesetz gerechtfertigt ist.

6.2 Verhältnismässigkeit

Die Datenerhebung muss erforderlich sein, zudem soll ein überwiegendes Interesse an der Erhebung bestehen. Datenerhebungen auf Vorrat sind widerrechtlich, nicht mehr benötigte Daten sind zu vernichten

6.3 Zweckbindung

Die Daten dürfen nur zu einem bestimmten, objektiv benötigten und für die betroffene Person erkennbaren Zweck bearbeitet werden. Sie dürfen nur zum Zweck bearbeitet werden, der bei der Erhebung der Daten genannt wurde.

6.4 Transparenz

Die Datenerhebung und -bearbeitung muss klar erkennbar sein. Die notwendigen Informationen werden nach Möglichkeit direkt bei der betroffenen Person beschafft werden.

6.5 Treu und Glauben

Widersprüchliches und rechtmissbräuchliches Verhalten sind unzulässig.

6.6 Datenqualität

Es muss sichergestellt sein, dass die bearbeiteten Daten richtig, vollständig und aktuell sind. Unrichtige und unvollständige Daten sind zu korrigieren oder zu vernichten.

7. Verantwortlichkeiten

7.1 Verwaltungsrat

Der Verwaltungsrat ist auf strategischer Ebene für die Gewährleistung des Datenschutzes im AZB verantwortlich.

Er nimmt den Datenschutz als relevantes Thema in sein Risk-Management auf und beurteilt die entsprechenden Risiken in strategisch stufengerechter Weise.

Er erlässt das vorliegende Datenschutzkonzept und überprüft dieses regelmässig.

Er regelt die Aufgaben, Verantwortlichkeiten und Kompetenzen der oder des DS-Verantwortlichen unter Berücksichtigung der Vorschriften der Gesetzgebung in der Funktionsbeschreibung der Geschäftsführerin oder des Geschäftsführers.

Er nimmt die regelmässige Berichterstattung der oder des DS-Verantwortlichen entgegen.

7.2 Geschäftsführerin bzw. Geschäftsführer als DS-Verantwortliche

Die oder der DS-Verantwortliche sorgt in geeigneter Weise dafür, dass alle Mitarbeitenden regelmässig für die Belange des Datenschutzes sensibilisiert und über die Vorgaben dieses Konzepts und deren Anwendung im beruflichen Alltag informiert werden.

Sie oder er nimmt betriebsintern die Aufgaben gemäss der Gesetzgebung und dem Pflichtenheft wahr.

Sie oder er ist nach innen und aussen die Ansprechperson für alle Fragen bezüglich des Datenschutzes.

Sie oder er prüft die Rechtmässigkeit der Datenbearbeitung im AZB.

Sie oder er erstattet gegebenenfalls Meldungen an die Datenschutzbeauftragten des Bundes und/oder des Kantons.

Sie oder er berichtet dem Verwaltungsrat jährlich über die Datenbearbeitung im AZB, weist dabei auf erkannte Risiken hin und gibt Empfehlungen für mögliche Verbesserungen ab. Über besondere Vorkommnisse von grösserer Tragweite orientiert sie oder er unverzüglich.

Sie oder er führt jährlich mit der oder dem Qualitätsbeauftragten Datenschutz-Audits durch.

7.3 Vorgesetzte

Die Vorgesetzten nehmen eine Vorbildfunktion wahr und fördern die Motivation der Mitarbeitenden, den Datenschutz bei ihrem Handeln am Arbeitsplatz einzuhalten.

Sie sind in ihren Verantwortungsbereichen für die Durchsetzung und Einhaltung des Datenschutzes verantwortlich, insbesondere im Rahmen dieses Konzepts und der Geschäftsprozesse.

Sie sorgen in Zusammenarbeit mit der oder dem DS-Verantwortlichen für die datenschutzmässige Sensibilisierung und handlungsorientierte Anleitung der Mitarbeitenden.

7.4 Mitarbeitende

Alle Mitarbeitenden des AZB, die Personendaten bearbeiten, tragen dem Datenschutz eigenverantwortlich Rechnung und handeln dabei insbesondere gemäss dem vorliegenden Konzept und den Weisungen der oder des DS-Verantwortlichen.

Sie wenden sich bei Fragen und Unsicherheiten an ihre Vorgesetzten oder an die oder den DS-Verantwortlichen

Mitarbeitende, die Kenntnis von einem Sicherheitsvorfall oder einer Datenschutzverletzung haben, melden dies unverzüglich der oder dem DS-Verantwortlichen.

8. Datensicherheit – Massnahmen

Mit organisatorischen und technischen Massnahmen müssen der Datenschutz gewährleistet und Personendaten insbesondere vor dem Zugang Unbefugter, Missbrauch, Vernichtung, Verlust, technischen Fehlern, Fälschung, Diebstahl usw. geschützt werden.

8.1 Organisatorische Massnahmen

Der Zugang zu Personendaten im AZB richtet sich nach dem Grundsatz «So viel wie nötig, so wenig wie möglich».

Die oder der DS-Verantwortliche regelt in Zusammenarbeit mit den jeweils zuständigen Bereichsleitenden für jede Datensammlung, wer unter welchen Bedingungen Zugang zu Personendaten hat und wie dies überwacht wird.

Sie oder er führt Bearbeitungsverzeichnisse gemäss den gesetzlichen Anforderungen und hält diese aktuell.

Sie oder er regelt zudem, wem Zugang zu archivierten Daten gewährt wird.

8.2 Technische Massnahmen

Der Schutz elektronisch bearbeiteter Daten wird insbesondere durch die Verwendung und regelmässige umfassende Verschlüsselung, den Einsatz von Firewalls, Virenschutzprogrammen usw. und die Protokollierung von Zugriffen gewährleistet. Der Vertrag mit CompuTech (externe IT-Firma) enthält die entsprechenden Bestimmungen.

Durch Zugangs- und Personendatenträgerkontrollen wird verhindert, dass unbefugte Personen Zugang zu Datenbeständen haben oder diese verändern, zerstören, entwenden usw.

8.3 Archivierung

Personendaten, die für die Bearbeitung nicht mehr benötigt werden, werden gemäss den Angaben der oder des DS-Verantwortlichen aufbereitet und während der definierten Dauer archiviert (Aufbewahrungsfristen s. Anhang 2).

8.4 Vernichtung

Daten von untergeordneter Bedeutung werden unmittelbar nach Erreichen des Bearbeitungszwecks vernichtet (physisch zerstört oder elektronisch unwiederbringlich gelöscht). Die oder der DS-Verantwortliche bestimmt die Einzelheiten.

9. Rechte der betroffenen Personen

9.1 Aufklärung/Orientierung

Bewohnerinnen, Bewohner sowie Mitarbeitende werden beim Eintritt über ihre datenschutzrechtlichen Rechte und Pflichten informiert.

Die oder der DS-Verantwortliche orientiert sie dabei angemessen über die Beschaffung der sie betreffenden Personendaten.

9.2 Auskunfts-/Einsichtsrecht

Die von der Bearbeitung ihrer Daten betroffene Person darf über Erhebung, Herkunft, Inhalt, Zweck, Kategorie und Rechtsgrundlage Auskunft verlangen und in die Datensammlung Einsicht nehmen. Sie hat auch das Recht auf die Bekanntgabe der an der Sammlung Beteiligten sowie der Datenempfängerinnen und -empfänger.

Die Auskunft oder Einsicht verlangende Person muss sich über ihre Identität ausweisen.

Bewohner, Bewohnerinnen, Kundinnen und Kunden haben das Recht, Vollmachten an Dritte zwecks Einsicht in ihre Daten zu vergeben. Angehörige sind Drittpersonen gleichgestellt.

Das Recht auf Einsichtnahme durch Dritte wird im Pensionsvertrag geregelt. Erteilte Vollmachten können jederzeit durch die die Vollmacht erteilende Person widerrufen werden. Eine schriftliche Vollmacht ist nicht notwendig, wenn die Angehörigen im Beisein der betroffenen Person Einsicht in die entsprechenden Daten nehmen.

Die Auskunft ist innert 30 Tagen in allgemeinverständlicher Weise, schriftlich und kostenlos zu erteilen.

Die Erteilung von Auskünften und die Einsichtsrechte dürfen ausnahmsweise beschränkt oder verweigert werden, wenn wichtige und überwiegende öffentliche Interessen oder besonders schützenswerte Interessen von Dritten entgegenstehen.

Besteht das Risiko, dass die betroffene Person (v.a. Minderjährige) mit der Auskunftserteilung oder Einsichtnahme einer zu hohen Belastung ausgesetzt werden könnte, kann sie eine andere Person bestimmen, der an ihrer Stelle Auskunft erteilt oder Einsicht gewährt wird.

9.3 Recht auf Berichtigung

Widerrechtlich oder unrichtig bearbeitete sowie unrichtige Daten müssen berichtigt oder vernichtet werden.

9.4 Sperrung/Verweigerung der Datenbekanntgabe

Jede betroffene Person kann die Bekanntgabe ihrer Daten sperren lassen, wenn sie ein schutzwürdiges Interesse nachweist. Dies gilt dann nicht, wenn die Datenbekanntgabe eine gesetzliche Verpflichtung darstellt, aufgrund überwiegender Interessen Dritter erforderlich ist oder zur Aufklärung von mutmasslich rechtsmissbräuchlichen Handlungen der betroffenen Person erforderlich ist.

10. Handlungsanweisungen für Mitarbeitende

10.1 Schweigepflicht

Mitarbeitende machen sich gemäss Ziffer 4.3 des Personalreglements sowie gemäss Artikel 35 DSG und Artikel 321a OR strafbar, wenn sie vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt geben, von denen sie bei der Ausübung ihres Berufes, der die Kenntnis solcher Daten erfordert, erfahren haben.

Diese Schweigepflicht ist Bestandteil des Arbeitsvertrages und gilt auch nach dem Austritt aus dem Betrieb. Zusätzlich ist jeder Mitarbeiter und jede Mitarbeiterin vor Stellenantritt verpflichtet, eine Vertraulichkeitserklärung zu unterschreiben.

10.2 Grundsätze zu Datenablage, -zugriff und –weitergabe

Daten sind ausschliesslich auf dem Server des AZB zu speichern. Die Datensicherung erfolgt täglich und extern durch CompuTech.

Die auf Papier festgehaltenen Bewohner-/Kundendaten sind durch technische und bauliche Massnahmen (z.B. Verschluss) vor unberechtigtem Zugriff durch Dritte zu schützen. Patientendossiers dürfen nicht unbeaufsichtigt und einsehbar herumliegen, elektronische Geräte dürfen für Unbefugte nicht zugänglich sein. Ebenso ist eine Bildschirmeinsicht durch Dritte zu verhindern.

10.3 Grundsätze der E-Mail-Nutzung

E-Mails können durch Dritte mitgelesen oder verändert werden. Grundsätzlich sollen deshalb nur ausnahmsweise Personendaten per E-Mail und nur an bekannte Adressatinnen und Adressaten übermittelt werden. Ist dies unumgänglich, dürfen sie keine sensiblen Informationen oder Angaben über Passwörter und andere Zugangsdaten enthalten.

Per E-Mail dürfen besonders schützenswerte Daten nur verschlüsselt übermittelt werden, sofern die betroffene Person keine gegenteilige, schriftliche Erklärung abgegeben hat.

Zu beruflichen Zwecken bearbeitete Personendaten dürfen nicht auf privaten Geräten gespeichert werden.

10.4 Verhalten bei telefonischen und schriftlichen Anfragen

Ohne ausdrückliche Einwilligung der betroffenen Person oder ohne entsprechende gesetzliche Erlaubnis dürfen Personendaten nicht an Aussenstehende weitergegeben werden.

Bei telefonischen Anfragen ist die eindeutige Identifizierung der anfragenden Person sicherzustellen.

10.5 Verwendung Bild-/Tonaufnahmen

Auf Bild-, Film- und/oder Tonaufnahmen erkennbar dürfen nur Personen festgehalten werden, die dazu ihre ausdrückliche Einwilligung gegeben haben.

Die Einwilligung der betroffenen Person muss freiwillig, ausdrücklich und nach vorgängiger Aufklärung über den Zweck und die Verwendung der Aufnahmen erfolgen. Die Zustimmung kann schriftlich oder – bei Anwesenheit mehrerer Personen – mündlich oder nonverbal erfolgen und ist zu dokumentieren.

In begründeten Fällen setzt das AZB Überwachungskameras ein. In diesem Fall müssen betroffene Personenkreise über Ort und den Zweck der Installation informiert werden.

11. Elektronisches Patientendossier (EPD)

11.1 Zugriff auf das EPD

Der Zugriff auf das EPD durch die berechtigten Personen darf nur auf Geräten des AZB erfolgen.

11.2 Organisation, Rollen und Aufgaben innerhalb des EPD

In der Richtlinie «EPD-Rollen und Zugriffsrechte“ des AZB sind die Organisationsstruktur und die entsprechenden Rollen in Bezug auf das EPD detailliert beschrieben.

11.3 Sicherheitsprozesse

Die Handhabung von Sicherheitsvorfällen wird gemäss HA_EPD-Sicherheitsvorfälle geregelt.

11.4 Behandlungsrelevante Dokumente

Im AZB sind folgende behandlungsrelevanten Dokumente für die Ablage im EPD vorgesehen:

- Medikamentenliste: Fixe Medikation und Reservemedikation
- Überweisungsbericht

11.5 Sensibilisierung und Schulung der Mitarbeitenden

11.5.1 Initiale Schulung

Die Qualitätsverantwortliche des AZB organisiert die initiale Schulung für sämtliche Mitarbeitende, die Zugriff auf das EPD erhalten. Die Schulungen werden in Form eines E-Learning durchgeführt und enthalten die Themen Datenschutz und Datensicherheit. Die Ergebnisse sowie die Bestätigungen der Durchführung des E-Learning werden im Dokument Schulungsnachweis gespeichert und bei Bedarf der DSDS-V der EPD-Stammgemeinschaft übergeben.

11.5.2 Wiederkehrende Schulungen

Alle EPD-Nutzerinnen und -Nutzer des AZB treffen sich einmal jährlich, um sicherheitsrelevante Themen zu besprechen. Die Organisation dieser Weiterbildungen (inkl. Anmeldung, Präsenzliste und Weiterbildungsnachweis) ist Aufgabe der DSDS-V des AZB. Bei Bedarf müssen die Weiterbildungsnachweise der EPD-Stammgemeinschaft übergeben werden.

11.6 Berichtswesen

Folgende Nachweise werden bei Bedarf der DSDS-V der EPD-Stammgemeinschaft abgegeben:

- Nachweis N00: Vertragseinhaltung (TOZ)
- Nachweis N01: Definition behandlungsrelevante Daten
- Nachweis N02: Dokumentation Prozess/Protokolle Notfallzugriff
- Nachweis N03: Dokumentation Konfiguration Endgeräte
- Nachweis N04: Dokumentation Patchmanagement
- Nachweis N05: Dokumentation Netzwerksicherheit
- Nachweis N06: Dokumentation Sicherheitsvorfälle
- Nachweis N07: Dokumentation Risikomanagement
- Nachweis N08: Reporting Sensibilisierung

12. Anhang 1

12.1 Abkürzungsverzeichnis

Abkürzung	Bedeutung
AZB	Alterszentrum Bremgarten
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
DSDS-V	Datenschutz- und Datensicherheitsverantwortliche Person (für EPD)
DS-Verantwortliche	Datenschutzverantwortliche Person im AZB (allgemein)
EPD	Elektronisches Patientendossier
EPD-Daten	Als EPD-Daten verstehen sich alle behandlungsrelevanten Daten oder Dokumente, welche im EPD-Kontext durch Patienten gemeinsam mit seinem Behandelnden in das EPD publiziert werden sollen. Im EPD sollen alle wichtigen Dokumente, die für einen weiteren Behandlungsverlauf relevant sind, zur Verfügung stehen.
TOZ	Technische- und Organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften.
XAD-SG	XAD-Stammgemeinschaft der Post Sanela Health AG

12.2 Begriffe

Begriff	Erläuterung
Personendaten	Angaben über eine bestimmte oder bestimmbare natürliche Person.
Besonders schützenswerte Personendaten	▪ Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; ▪ Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer ethnischen Gruppe oder Herkunft; ▪ genetische Daten; ▪ biometrische Daten, die eine natürliche Person eindeutig identifizieren; ▪ Daten über verwaltungs- und strafrechtliche Verfolgung oder Sanktionen; ▪ Daten über Massnahmen der sozialen Hilfe.
Bearbeiten von Personendaten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, wie das Beschaffen, Speichern, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.
Bekanntgabe von Personendaten	Jedes Übermitteln oder Zugänglichmachen von Personendaten.
Datensammlung	Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach bestimmten Personen erschliessbar sind.
Datenschutzverantwortliche Person	Person, welche betriebsintern die Einhaltung der Datenschutzvorschriften überwacht und u.a. ein Verzeichnis der Datensammlungen führt.
Inhaber/in der Datensammlung	Verantwortliche/r für eine Datenbearbeitung. Sie/Er entscheidet allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung.
Persönlichkeitsprofil	Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
Profiling	Bewertung bestimmter Merkmale einer Person aufgrund von automatisiert bearbeiteten Personendaten (um z.B. die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, bestimmte Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen).

13. Anhang 2

Aufbewahrungsfristen / Allgemeine Verjährungsfristen gemäss Bundesrecht
(Zusammenstellung von Curaviva, April 2023)

Gegenstand	(längste) Verjährungsfrist	gesetzliche Grundlage	Bemerkungen
Geschäftsbücher, Geschäftsbericht, wichtige Belege für Buchhaltung	10 Jahre	Art. 957ff. OR	Die Buchführungspflicht «erfasst diejenigen Geschäftsvorfälle und Sachverhalte, die für die Darstellung der Vermögens-, Finanzierungs- und Ertragslage des Unternehmens (wirtschaftliche Lage) notwendig sind» (Art. 957a Abs. 1 OR). Aufzubewahren sind insbesondere Geschäftsbücher und Buchungsbelege, wozu unter Umständen auch Geschäftskorrespondenz im Zusammenhang mit einem Geschäftsvorfall gehört. Wichtige Belege können unter Umständen auch Arbeits- und Heimverträge sein.
Allgemeine arbeitsrechtliche Ansprüche	5 Jahre	Art. 128 OR	
Daten mit Relevanz für Arbeitszeugnis	10 Jahre		Frist gemäss Rechtsprechung
Lohndaten und arbeitsrechtliche Dokumente mit steuerrechtlicher Relevanz	10 Jahre	Art. 958f Abs. 1 OR; Art. 126 Abs. 3 DBG	
Dokumentation der Einhaltung von Pflichten gemäss Arbeitsgesetz (insbesondere Arbeitszeitkontrollen)	5 Jahre	Art. 73 Abs. 2 Verordnung 1 zum Arbeitsgesetz	
Schadenersatz/Genugtuung bei Körperverletzung/Tötung eines Menschen	3/20 Jahre	Art. 60 Abs. 1bis und Art. 128a OR	Kann frühere Mitarbeitende und ehemalige Klient:innen betreffen
Geschlechtsdiskriminierende Verstösse	3 Monate	Art. 8 Abs. 2 Gleichstellungsgesetz	
Leistungen von oder Beiträge an Sozialversicherungen bzw. Pflicht zu deren Rückerstattung	5 Jahre	Art. 24 und 25 ATSG	Bei *Unfällen* während Arbeitsverhältnis wird jedoch Aufbewahrung der Personalakten während 10 Jahren, bei schweren Unfällen oder Berufskrankheiten während 30 Jahren empfohlen (ad hoc-Empfehlung UVG Nr. 09/87; https://www.koordination.ch/fileadmin/files/ad-hoc/1987/09-87.pdf)