Datenschutz- und Informationssicherheitsrichtlinie

1 Ziel

Die Datenschutzgesetze und die Interessen unserer Bewohner, Mitarbeiter und Geschäftspartner verlangen eine Sicherstellung der Vertraulichkeit der Personendaten. Der Schutz von Personendaten ist deshalb für den Gemeindeverband Regionale Alterszentren von wesentlicher Bedeutung.

Diese Datenschutzrichtlinie bezweckt den Schutz der Persönlichkeit sowie der Grundrechte von Personen in Bezug auf die Bearbeitung ihrer Personendaten durch Mitarbeitende des Gemeindeverbandes.

2 Gesetzliche Grundlagen

Diese Datenschutzrichtlinie richtet sich nach den Bestimmungen der Datenschutzgesetze des Bundes und des Kantons Aargau. Dies sind:

- Bundesgesetz über den Datenschutz (DSG; SR 235.1)
- Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11)
- Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen des Kantons Aargau (IDAG; SAR 150.700)
- Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen des Kantons Aargau (SAR 150.711).

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen (insbesondere im Gesundheitsrecht) zu beachten.

Im Bereich des privatwirtschaftlichen Handelns untersteht der Gemeindeverband Regionale Alterszentren grundsätzlich der Datenschutzgesetzgebung des Bundes.

Soweit der Gemeindeverband Regionale Alterszentren Leistungen im Zusammenhang mit der Grundversicherung erbringt bzw. einen kantonalen Leistungsauftrag erfüllt, sind die Bestimmungen des kantonalen Datenschutzgesetzes anwendbar.

3 Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter des Gemeindeverbandes Regionale Alterszentren. Sie gilt für jede Bearbeitung von Personendaten, unabhängig davon, ob Personendaten in Schriftstücken enthalten oder elektronisch gespeichert, oder ob sie manuell oder unter Einsatz elektronischer Geräte bearbeitet werden.

4 Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

Die Geschäftsleitung ist für die gesetzeskonforme Bearbeitung von Personendaten verantwortlich. Sie sorgt dafür, dass durch organisatorische, personelle und technische Massnahmen eine ordnungsgemässe Datenbearbeitung unter Beachtung des Datenschutzes und der Informationssicherheit eingehalten werden.

4.2 Datenschutzbeauftragter

Der / die Datenschutzbeauftragte ist verantwortlich für die Überwachung der Einhaltung der Datenschutzvorschriften. Er / sie übt ihre / seine Funktion fachlich unabhängig und weisungsungebunden aus.

Der / die Datenschutzbeauftragte ist Ansprechpartner für den Datenschutz. Er / sie berät die Geschäftsleitung sowie die Mitarbeitenden des Gemeindeverbandes Regionale Alterszentren zu den Pflichten nach den Datenschutzvorschriften und unterrichtet die Geschäftsleitung zeitnah über Datenschutzrisiken.

Bei Datenschutzkontrollen bzw. Anfragen von Aufsichtsbehörden ist der / die Datenschutzbeauftragte umgehend zu informieren.

Der / die Datenschutzbeauftragte kann wie folgt erreicht werden:

Gemeindeverband Regionale Alterszentren
Datenschutzbeauftragte
Zugerstrasse 6 / Postfach 931
5620 Bremgarten
Telefon: 056 649 22 22
E-Mail: roger.cebe@alterszentren.ch

4.3 Mitarbeiterinnen und Mitarbeiter

Alle Mitarbeitenden des Gemeindeverbandes Regionale Alterszentren sind bei ihrer Arbeit mit Personendaten für den korrekten Umgang mit diesen Daten verantwortlich. Sie beachten bei der Bearbeitung von Personendaten insbesondere die Datenschutzgrundsätze gemäss Ziffer 6 dieser Datenschutzrichtlinie.

Sie unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben, indem sie ihm auf Anfrage Zugang zur Personendaten und Bearbeitungsvorgängen gewähren, Auskünfte erteilen oder Unterlagen aushändigen.

Jeder Mitarbeiter meldet einen Datenschutzvorfall sowie jeden konkreten Verdacht auf einen Datenschutzvorfall gemäss Ziffer 11 dieser Datenschutzrichtlinie sofort intern an den Datenschutzbeauftragten.

5 Begriffe

Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. *Auch Angaben, die keinen Namen enthalten, sind Personendaten, wenn mit Hilfe von Zusatzinformationen realistischerweise eine Zuordnung zu einer natürlichen Person möglich ist (z.B. Liste mit Benutzerkennung und System-Anmeldezeiten kann problemlos einem Mitarbeiter zugeordnet werden). Auch im Geschäftsverkehr liegen personenbezogene Daten vor, etwa Kontaktdaten von Ansprechpartnern (z.B. Herr Robert Müller arbeitet im Einkauf der XY AG).*

besonders schützenswerte Personendaten	Daten, bei denen aufgrund ihrer Bedeutung, des Zusammenhangs, Zwecks oder der Art der Bearbeitung, der Datenkategorie oder anderer Umstände eine besondere Gefahr einer Persönlichkeitsverletzung besteht. *Dies sind namentlich, 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.*
betroffene Person	Natürliche Person, über die Personendaten bearbeitet werden (*z.B. Mitarbeiter, Bewohner, Kunde oder Ansprechpartner beim Lieferanten*).
Bearbeiten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.
Bekanntgeben	Das Übermitteln oder Zugänglichmachen von Personendaten (z.B. *das Einsichtsgewähren, Weitergeben oder Veröffentlichen)*.
Profiling	Jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
Profiling mit hohem Risiko	Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
Verletzung der Datensicherheit	Eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.
Verantwortlicher	natürliche Person oder Unternehmen, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.
Auftragsbearbeiter	natürliche Person oder Unternehmen, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

6 Allgemeine Grundsätze für die Datenbearbeitung

6.1 Rechtmässigkeit

Die Bearbeitung von Personendaten greift immer in die Grundrechte der betroffenen Person ein. Personendaten dürfen durch den Gemeindeverband Regionale Alterszentren nur rechtmässig bearbeitet werden, also nicht in Verletzung einer anderen gesetzlichen Norm, welche direkt oder indirekt den Schutz der Persönlichkeit bezweckt.

6.1.1 Datenbearbeitung aufgrund gesetzlicher Erlaubnis oder Pflicht

Die Bearbeitung von Personendaten ist zulässig, wenn Rechtsvorschriften die Datenbearbeitung verlangen (z.B. Pflegedokumentation), voraussetzen oder gestatten. Die Art und der Umfang der Datenbearbeitung müssen für die gesetzlich zulässige Datenbearbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

6.1.2 Datenbearbeitung für eine vertragliche Beziehung

Personendaten der betroffenen Person dürfen zur Begründung, Durchführung und Beendigung eines Vertrages (z.B. Arbeitsvertrages) bearbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht.

6.1.3 Einwilligung in die Datenbearbeitung

Eine Datenbearbeitung kann aufgrund einer Einwilligung der betroffenen Person stattfinden. Vor der Einwilligung muss der Betroffene gemäss Ziffer 12.1 dieser Datenschutzrichtlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen.

6.2 Verhältnismässigkeit

Personendaten dürfen durch den Gemeindeverband Regionale Alterszentren bearbeitet werden, wenn die Bearbeitung verhältnismässig, das heisst für die Aufgabenerfüllung geeignet und erforderlich ist. Dies ist bereits beim Umfang der Datenerhebung zu berücksichtigen.

Sofern der Zweck es zulässt und der Aufwand in einem angemessenen Verhältnis zu dem verfolgten Ziel steht, sind anonymisierte oder statistische Daten zu verwenden.

6.3 Zweckbindung

Personendaten dürfen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden.

Der Gemeindeverband Regionale Alterszentren gewährleistet, dass Personendaten zu einem nicht personenbezogenen Zweck (z.B. Forschung, Planung und Statistik) nur bearbeitet werden, wenn diese anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind.

6.4 Richtigkeit der Daten

Personendaten müssen richtig und, soweit es der Zweck des Bearbeitens verlangt, vollständig sein. Die Beweislast für die Richtigkeit der Personendaten trägt der Gemeindeverband Regionale Alterszentren.

Unrichtige oder unvollständige Personendaten müssen unverzüglich gelöscht, korrigiert, ergänzt oder aktualisiert werden.

6.5 Transparenz

Die Beschaffung von Personendaten und der Zweck ihrer Bearbeitung durch den Gemeindeverband Regionale Alterszentren müssen für die betroffenen Personen erkennbar sein (d.h. keine heimliche Beschaffung). Grundsätzlich sind Personendaten bei dem Betroffenen selbst zu erheben.

6.6 Vernichtung und Anonymisierung

Personendaten müssen vernichtet bzw. gelöscht oder anonymisiert werden, sobald sie zum Zweck ihrer Bearbeitung nicht mehr erforderlich sind, ausser wenn ein Gesetz eine längere Aufbewahrungsfrist verlangt.

7 Datensicherheit

Der Gemeindeverband Regionale Alterszentren schützt Personendaten vor unbefugtem Zugriff und unrechtmässiger Bearbeitung oder Weitergabe sowie gegen Verlust, Veränderung oder Zerstörung mit angemessenen technischen und organisatorischen Datensicherheitsmassnahmen. Diese Massnahmen müssen auf dem Stand der Technik, den Risiken der Bearbeitung und dem Schutzbedarf der Personendaten beruhen.

8 Datenschutz-Folgenabschätzung

Der Gemeindeverband Regionale Alterszentren analysiert bei der Einführung neuer Bearbeitungsvorgänge oder bei einer wesentlichen Änderung eines bestehenden Bearbeitungsvorganges vor der Bearbeitung, insbesondere durch die Verwendung neuer Technologien, ob diese Bearbeitung ein hohes Risiko für die Grundrechte der Betroffenen darstellt. Dabei sind Art, Umfang, Kontext und Zweck der Datenbearbeitung zu berücksichtigen.

Im Rahmen der Risikoanalyse führt der Gemeindeverband Regionale Alterszentren eine Bewertung der Auswirkungen der geplanten Bearbeitungen auf den Schutz von Personendaten durch (Datenschutz-Folgenabschätzung).

Besteht nach Durchführung der Datenschutz-Folgenabschätzung und der Anwendung geeigneter Massnahmen zur Risikominderung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen, muss der / die Datenschutzbeauftragte die zuständige Datenschutzaufsichtsbehörde konsultieren (Vorab-Konsultation).

9 Verzeichnis der Bearbeitungstätigkeiten

Der Gemeindeverband Regionale Alterszentren dokumentiert alle Bearbeitungstätigkeiten, in denen Personendaten bearbeitet werden, in einem Verzeichnis. Das Verzeichnis ist schriftlich zu führen und enthält die datenschutzrechtlich wesentlichen Eckwerte der Datenbearbeitungen (jedoch keine Personendaten).

10 Bearbeitung im Auftrag

10.1 Allgemeines

Eine Auftragsbearbeitung liegt vor, wenn ein Auftragnehmer Personendaten im Namen und nach Weisung des Gemeindeverbandes Regionale Alterszentren (Auftraggeber) bearbeitet. In diesen Fällen ist eine Vereinbarung über eine Auftragsbearbeitung abzuschliessen gemäss den einschlägigen gesetzlichen Anforderungen. Der Gemeindeverband Regionale Alterszentren trägt die volle Verantwortung für die korrekte Durchführung der Datenbearbeitung.

10.2 Bestimmungen für Auftraggeber (Gemeindeverband Regionale Alterszentren)

Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten:

- Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmassnahmen auszuwählen;
- Der Auftrag ist schriftlich zu erteilt. Die Vorgaben zur Datenbearbeitung und die Verantwortlichkeiten sind zu dokumentieren;
- Der Gemeindeverband Regionale Alterszentren muss sich vor Beginn der Datenbearbeitung durch geeignete Prüfung vergewissern, dass der Auftragnehmer die vorgenannten Pflichten erfüllt. Ein Auftragnehmer kann seine Einhaltung der Datenschutzanforderungen insbesondere durch eine entsprechende Zertifizierung dokumentieren. Je nach Risiko der Datenbearbeitung müssen Prüfungen während der Vertragslaufzeit regelmässig wiederholt werden;
- Eine grenzüberschreitende Auftragsdatenbearbeitung ist nur zulässig, wenn der Auftragnehmer ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau nachweist.

10.3 Bestimmungen für Auftragnehmer

Der Auftragnehmer darf Personendaten nur im Rahmen der Weisungen des Gemeindeverbandes Regionale Alterszentren als Auftraggeber bearbeiten.

Der Auftragnehmer darf Dritte («Unterauftragnehmer») zur Bearbeitung von Personendaten im eigenen (Unternehmen) den Auftrag nur mit vorherigem Einverständnis des Gemeindeverbandes Regionale Alterszentren beauftragen. Das Einverständnis darf nur erteilt werden, wenn der Auftragnehmer dem Unterauftragnehmer vertraglich die gleichen Datenschutzpflichten, die dem Auftragnehmer nach Massgabe dieser Richtlinie gegenüber dem Gemeindeverband Regionale Alterszentren und den Betroffenen obliegen, und angemessene technische und organisatorische Schutzmassnahmen auferlegt. Die Form des Einverständnisses sowie Informationspflichten bei Änderungen im Unterauftragsverhältnis sind im Dienstleistungsvertrag zu regeln.

11 Verletzung der Datensicherheit

Eine Verletzung der Datensicherheit (Datenschutzvorfall) liegt vor, wenn Personendaten unwiederbringlich vernichtet werden bzw. verloren gehen, oder unbeabsichtigt oder unrechtmässig verändert bzw. offenbart werden oder Unbefugten zugänglich werden.

11.1 Interne Meldepflicht

Wurde eine Datenschutzverletzung festgestellt oder vermutet, ist jeder Mitarbeiter verpflichtet, dies unverzüglich dem Datenschutzbeauftragten mitzuteilen, insbesondere bei schwerwiegenden Datenschutzverletzungen und solchen, bei denen zum Schutz der Betroffenen Schutzmassnahmen durch den Gemeindeverband Regionale Alterszentren getroffen werden müssen.

Die Meldung kann in jeder Form erfolgen; bei mündlichen Meldungen sind diese unverzüglich schriftlich nachzuholen.

11.2 Nachforschung und Sicherheitsmassnahmen

Handelt es sich bei der Meldung um einen Verdacht einer Verletzung der Datensicherheit, leitet der /die Datenschutzbeauftragte unverzüglich etwaig erforderliche Nachforschungsmassnahmen ein und informiert unverzüglich die Geschäftsleitung. Gleiches gilt, wenn die wahrscheinlichen Folgen der Datenschutzverletzung und damit das mögliche Risiko der Datenschutzverletzung unklar sind.

Soweit erforderlich leitet der Datenschutzbeauftragte bzw. die Geschäftsleitung sofort Massnahmen (z.B. Sperrung von Zugängen, Änderung von Passwörtern, Einspielen von Backups) zur Behebung der Datenschutzverletzung oder zur Abmilderung möglicher nachteiliger Auswirkungen der Verletzung der Datensicherheit.

11.3 Meldung an die Datenschutz-Aufsichtsbehörde

Der Datenschutzbeauftragte muss entsprechende Ereignisse unverzüglich der zuständigen Aufsichtsbehörde melden, wenn die Verletzung der Datensicherheit zu einer Gefährdung der Grundrechte auf informationelle Selbstbestimmung bzw. auf Privatsphäre von betroffenen Personen führen kann. Bestehen Zweifel, ob Grundrechte der Betroffenen gefährdet sind, ist ebenfalls Meldung zu erstatten.

11.4 Benachrichtigung von Betroffenen

Zusätzlich müssen die Betroffenen benachrichtigt werden, wenn es zu deren Schutz erforderlich ist. Für die Benachrichtigung ist der Datenschutzbeauftragte verantwortlich, der sich hierzu mit der Geschäftsleitung abstimmt.

12 Rechte der Betroffenen

Der Gemeindeverband Regionale Alterszentren hat durch geeignete technische und/oder organisatorische Massnahmen sicherzustellen, dass die Rechte der Betroffenen, in der Regel innert 30 Tagen, erfüllt werden können.

12.1 Informationspflicht

Bei Beschaffung von Personendaten werden der betroffenen Person mindestens die Kontaktdaten des Gemeindeverbandes Regionale Alterszentren, der Bearbeitungszweck, gegebenenfalls die Empfänger oder die Kategorien von Empfängern, denen Personendaten bekanntgegeben werden sowie die Rechte der betroffenen Person mitgeteilt.

Die Informationspflicht entfällt, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt oder die Bearbeitung gesetzlich vorgesehen ist.

12.2 Auskunfts- und Einsichtsrechte

Betroffene können Auskunft verlangen, ob über sie Personendaten bearbeitet und wenn dies der Fall ist, welche Datenkategorien für welche Zwecke bearbeitet werden.

IT-Systeme sind so auszuwählen bzw. zu gestalten, dass zur Erfüllung des Auskunftsrechts alle Angaben über die Betroffenen ausgedruckt werden können, oder es wird durch ein Verfahren sichergestellt, dass alle Angaben zu einer Person manuell aus dem System extrahiert werden können.

12.3 Recht auf Berichtigung

Betroffene können Berichtigung oder Ergänzung ihrer Personendaten verlangen.

Unrichtige Personendaten müssen unverzüglich berichtigt und – soweit der Zweck der Bearbeitung dies erfordert – unvollständige Personendaten ergänzt werden.

12.4 Recht auf Vernichtung

Betroffene sind berechtigt, Vernichtung bzw. Löschung ihrer Personendaten zu verlangen.

Wenn Personendaten unrechtmässig erhoben wurden oder die Personendaten für den Zweck, für den sie erhoben oder sonst bearbeitet werden, nicht mehr benötigt werden, sind diese zu vernichten bzw. zu löschen. Bestehende gesetzliche Aufbewahrungspflichten und einer Vernichtung- bzw. Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

13 Sensibilisierung und Schulung

Alle Führungskräfte müssen sicherstellen, dass ihre Mitarbeiter über die erforderlichen Datenschutzkenntnisse verfügen, soweit sie ständigen oder regelmässigen Zugang zu Personendaten haben oder an der Bearbeitung von Personendaten beteiligt sind.

Für die Durchführung bzw. Bereitstellung der Schulungen zum Datenschutz ist der Datenschutzbeauftragte verantwortlich. Er konzipiert inhaltlich die Datenschutzschulungen und legt die Kriterien für den Teilnehmerkreis fest.

14 Datenschutzkontrolle

Die Einhaltung dieser Richtlinie und der geltenden Datenschutzgesetze wird im Gemeindeverband Regionale Alterszentren regelmässig, mindestens einmal jährlich, risikobasiert überprüft. Die Durchführung obliegt dem Datenschutzbeauftragten. Die Ergebnisse der Datenschutzkontrollen sind im Wesentlichen der Geschäftsleitung mitzuteilen.

15 Sanktionen

Eine missbräuchliche Bearbeitung von Personendaten oder andere Verstösse gegen das Datenschutzgesetz können strafrechtlich verfolgt werden und Schadenersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können auch zu arbeitsrechtlichen Sanktionen führen.