KANTON AARGAU

DEPARTEMENT
GESUNDHEIT UND SOZIALES
Abteilung Gesundheit

9. Januar 2020

Organisationsinterne Datenschutz- und Datensicherheits-Regelung

---

Anleitung
Wo gelb markiert → Angaben der Spitexorganisation einsetzen.

Stand des Dokuments

Version Nr.	Bearbeitet am	Bearbeitet/beschlossen durch	Status

In der Tabelle sollte jeweils auch der geplante künftige Überprüfungszeitpunkt eingefügt werden

1. Name der Spitexorganisation

Das nachfolgende Datenschutz- und Datensicherheitskonzept wird im Anhang zu den Vorgaben Datenschutz für Organisationen der Hilfe und Pflege zu Hause (Spitexorganisationen) erlassen.

Es gilt in Konkretisierung der Datenschutzgesetzgebung und der Vorgaben Datenschutz für

(Variante 1: Alle Betriebsstandorte der [Name der Spitexorganisation])

(Variante 2: Den Stützpunkt [Bezeichnung des Stützpunkts] der Name der Spitexorganisation])

2. Bezeichnung und Adressen der kommunal zuständigen Verantwortlichen

(Gemeinde: Name der Gemeinde)

(Bezeichnung der Behörde, zum Beispiel Gemeinderat)

(Postadresse der Behörde)

(Ansprechperson mit Telefon Nr., zum Beispiel Kommissionspräsident/in, Gemeindeschreiber/in)

3. Zugangsberechtigung nach Funktionen (operativ zuständige Personen)

Die Zugangsberechtigung zu den Datensammlungen mit Personendaten wird wie folgt festgelegt:

Bezeichnung der Datensammlung	Funktionsbezeichnung der zuständigen Berechtigten

Hinweis: Die Auflistung der Datensammlungen bezweckt, einen kompetenzgerechten, geordneten Zugang zu den verschiedenen Datensammlungen innerhalb der Organisation sicherzustellen.

Beispiel (Illustration zum Ausfüllen der vorstehenden Tabelle)

Bezeichnung der Datensammlung	**Funktionsbezeichnung (bei kleinen Organisationen Vornamen und Namen) der Berechtigten**
Klientendossiers (inklusive mobile Geräte wie Tablets, Ausdrucke usw.)	Die mit einer Aufgabenerfüllung gegenüber der Klientin oder dem Klienten betrauten Pflegenden (inkl. Auszubildende) jeweils vor Ort bei der Klientin/beim Klienten
Elektronisch oder physisch geführtes Archiv der Klientendossiers	Betriebsleiter/in Buchhalter/in
Kreditorenliste der Finanzbuchhaltung	Betriebsleiter/in Buchhalter/in Revisionsstelle (bei der Revision)
Rechnungs- und Mahnungskopien	Betriebsleiter/in Buchhalter/in Revisionsstelle (bei der Revision)
Elektronische oder physische Personaldossiers	Betriebsleiter/in Geschäftsleitung
Weiteres	

4. Datensicherung

Die Datensicherung wird – gegliedert nach Datensammlungen – wie folgt durchgeführt:

Bezeichnung der Datensammlung	**Beschreibung der Sicherungsmassnahme**	**Verantwortliche Person (Stellvertretung)**
		(Vorname, Name) (Vorname, Name)
		(Vorname, Name) Vorname, Name)

Beispiel (Illustration zum Ausfüllen der vorstehenden Tabelle)

Bezeichnung der Datensammlung	Beschreibung der Sicherungsmassnahme	Verantwortliche Person (Stellvertretung)
Klientendossiers	Elektronische Dossiers: Berechtigungskonzept; Zugriff nur durch die berechtigten Personen mittels sicherem Passwort (wird regelmässig geändert). Regelmässiges Backup, Schutz durch Firewall. Physische Dossiers: Berechtigungskonzept; Zugriff nur durch die berechtigten Personen. Nach Gebrauch die physisch vorhandenen Dossiers immer in die vereinbarte Schublade/den vereinbarten Schrank wegsperren	Alle Pflegenden
Archiv	Elektronische Dossiers: Berechtigungskonzept; Zugriff nur durch die berechtigten Personen mittels sicherem Passwort (wird regelmässig geändert). Regelmässiges Backup, Schutz durch Firewall. Physische Dossiers: Berechtigungskonzept; Zugriff nur durch die berechtigten Personen. Nach Gebrauch die physisch vorhandenen Dossiers immer in die vereinbarte Schublade/den vereinbarten Schrank wegsperren	Betriebsleiter/in Buchhalter/in
Datensicherung	Automatische Datensicherung des Servers (alle 12 Stunden) Sicherungskopie Monatsabschluss auf externen Datenträger; dieser wird im Safe eingeschlossen	XY (ZZ)

Alle Geräte, die einen Zugang zu Klienten- oder Personaldaten ermöglichen, werden unter Verschluss gehalten (Türen abschliessen, Notebooks in Schränken einschliessen etc.).

5. E-Mail-Verkehr mit besonders schützenswerten Personendaten

Für die Übermittlung von besonders schützenswerten Personendaten (zum Beispiel Pflegedokumentationen oder Personalakten) ist eine HIN-Mailadresse oder eine gleichwertig sichere Mailadresse zu installieren und zu verwenden.

6. Passwörter

Grundregeln

- PC- und Notebook-Arbeitsplätze werden generell durch Passwort geschützt

- Passwörter müssen aus mindestens 8 Zeichen bestehen (sinnvollerweise Buchstaben, Zahlen, Sonderzeichen)
- Passwörter müssen vierteljährlich geändert werden
- Umgang mit mobilen Geräten wie Tablets muss geregelt werden (Passwortschutz, Aufbewahrung nach Gebrauch usw.)

Zuständigkeit zur Passwortvergabe (Neuvergabe oder Änderung bei Verlust):

(Funktion)

7. Archivierung

Die Archivierung erfolgt gemäss den Vorgaben des aargauischen Gesundheitsgesetzes. Das heisst, die Originaldossiers werden während mindestens 10 Jahren seit Erstellung in elektronischer Form aufbewahrt und mittels technischen Schutzmassnahmen gegen unbefugten Zugriff geschützt und abgesichert. Unter Beachtung der Verlängerung der Verjährungsfrist für Forderungen aus unerlaubten (Art. 60 OR) oder vertragswidrigen Handlungen (Art. 128a OR) bei Körperschäden und Todesfällen ist zu empfehlen, Patientenakten 20 Jahre aufzubewahren. Physische Originaldossiers werden gesondert an einem verschlossenen und geschützten Ort aufbewahrt.

8. Aufbewahrung der Daten bei einer allfälligen Auflösung der Spitexorganisation

Die Aufbewahrung der Daten bei einer Fusion mit einer anderen Spitexorganisation wird im Fusionsvertrag geregelt.

Bei der ersatzlosen Auflösung der Spitexorganisation entscheidet die zuständige Gemeinde als Vertragspartnerin der Leistungsvereinbarung über den sicheren Verbleib der Daten. Die gesetzlichen Aufbewahrungsfristen sind einzuhalten.

9. Checkliste zur Schulung der Mitarbeitenden hinsichtlich des Datenschutzes

Verantwortlich für die Schulung beziehungsweise Einführung von neuen Mitarbeiterinnen und Mitarbeitern (Pflegende und andere) ist die betreffende Spitexorganisation, welche eine Mitarbeiterin/einen Mitarbeiter für die Schulung beziehungsweise Einführung von neuen Mitarbeiterinnen und Mitarbeitern bestimmt.

Die Schulung umfasst namentlich die Einführung der neuen Mitarbeitenden in die Vorgaben Datenschutz, in die vorliegende Datenschutz- und Datensicherheits-Regelung sowie in das Berufsgeheimnis. Die praktische Handhabung der Klientendossiers wird mit einer erfahrenen Person eingeübt.

Olga Hürlimann
Fachspezialistin Pflege ambulant