



Leitfaden

Datenschutz im Bereich der sozialen Einrichtungen

Personen, die in Kinder- und Jugendheimen, Betagten- und Pflegeheimen sowie Einrichtungen für Menschen mit Behinderung arbeiten, haben täglich mit sensiblen Personendaten zu tun. Der Schutz der Persönlichkeit der Klientinnen und Klienten ist dabei ein wichtiges Thema. Dieser Leitfaden umfasst sowohl die Grundlagen des Datenschutzes als auch Antworten bzw. praxisbezogene Empfehlungen auf häufig gestellte Fragen zum Umgang mit Personendaten in den erwähnten Einrichtungen.

Der Leitfaden richtet sich an private und öffentliche Trägerschaften folgender Angebote:

- Kinder- und Jugendheime
- Stationäre Einrichtungen für Menschen mit Behinderung
- Betagten- und Pflegeheime

Zugelassene oder anerkannte private Einrichtungen, die über einen Leistungsauftrag des Staates verfügen und ihre Leistungen abgegolten erhalten, haben in Bezug auf den Datenschutz die kantonalen Vorgaben für öffentliche Organe zu erfüllen, da sie Staatsaufgaben erfüllen. Für übrige Privatpersonen ist im Umgang mit Personendaten das Bundesrecht massgeblich.¹

4. April 2019

¹ Vgl. Leitfaden für die Bearbeitung von Personendaten im medizinischen Bereich, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Juli 2002: www.edoeb.admin.ch → Datenschutz → Dokumentation → Leitfäden.

Inhalt

1	Grundlagen des Datenschutzes	3
1.1	Was ist Datenschutz?	3
1.2	Begriffe	3
1.3	Grundsätze	4
1.4	Datenbearbeitung	5
1.5	Rechte der betroffenen Person	6
2	Häufige Fragen	7
2.1	Datenbearbeitung und Aktenführung	7
2.2	Datenbekanntgabe: Auskunft an und Einsicht durch Drittpersonen	10
2.3	Recht der betroffenen Personen auf ihre persönlichen Daten	12
2.4	Aufbewahrung und Archivierung von Klientendossiers	12
2.5	Informationssicherheit	13
3	Kontakt	14
4	Weiterführende Links	14

1 Grundlagen des Datenschutzes²

1.1 Was ist Datenschutz?

Der Datenschutz regelt, was datenschutzrechtlich bei der Bearbeitung von Personendaten zu beachten ist (vgl. Ziff. 1.4). Zweck ist der Schutz der Persönlichkeit von Personen, über die Daten bearbeitet werden. Es handelt sich um ein Grundrecht, das jedem Menschen zusteht.

1.2 Begriffe

1.2.1 Was sind Personendaten?

Personendaten sind Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.³

Beispiele:

- Adressen
- Personalien von Mitarbeitenden oder Klientinnen und Klienten
- Fotos von Mitarbeitenden oder Klientinnen und Klienten

1.2.2 Was sind besonders schützenswerte Personendaten?

Dies sind Angaben über:

- a. religiöse, weltanschauliche sowie politische Ansichten und Tätigkeiten (ausgenommen sind Angaben über die Mitgliedschaft bei einer Religionsgemeinschaft, einer Organisation, einer politischen Partei, wenn die betroffene Person diese selbst bekannt gegeben hat oder für ein öffentliches Amt kandidiert);
- b. Gesundheit, Intimsphäre und Rassenzugehörigkeit;
- c. Leistungen und Massnahmen der sozialen Hilfe;
- d. strafrechtliche sowie disziplinarische Verfahren und Sanktionen.

² Es werden die gesetzlichen Bestimmungen des [Datenschutzgesetzes des Kantons St.Gallen](#) (sGS 142.1; abgekürzt DSG) angewendet. Aktuell berät der Kantonsrat einen Nachtrag zum Datenschutzgesetz (ABI 2018, 4049). Aufgrund der Änderungen wird dieses Merkblatt Anfang 2020 überarbeitet.

³ Art. 1 Abs. 1 Bst. a DSG.

1.2.3 Was ist ein Persönlichkeitsprofil?

Ein Persönlichkeitsprofil ist eine Zusammenstellung von Personendaten, welche die Beurteilung der Persönlichkeit einer natürlichen Person⁴ erlaubt.

Beispiele:

- Bewerbungsmappe
- Krankengeschichte
- Klientendossier

1.2.4 Wer ist die betroffene Person?

Die betroffene Person ist in der Regel eine natürliche Person, über die Personendaten bearbeitet werden, also eine betreute oder angestellte Person.⁵

1.3 Grundsätze

Das Datenschutzrecht kennt verschiedene Grundsätze:

Grundsatz der Rechtmässigkeit

Die Datenbearbeitung muss rechtmässig sein. Das heisst, es wird ein Rechtfertigungsgrund benötigt, entweder in Form einer Einwilligung der betroffenen Person, eines überwiegenden öffentlichen oder privaten Interesses oder eines Gesetzes.

Grundsatz der Verhältnismässigkeit

Die Datenbearbeitung muss verhältnismässig sein, d.h. die bearbeiteten Daten müssen geeignet und erforderlich sein, um den definierten Zweck zu erfüllen. Zudem muss der angestrebte Zweck den Eingriff in die Persönlichkeitsrechte rechtfertigen.

Beispiel:

Für die Betreuung einer Person wird ein Klientendossier angelegt. Es sind diejenigen Angaben aufzunehmen, die für den Abschluss eines Betreuungsvertrags und die Wahrnehmung des damit verbundenen Betreuungsauftrags der Einrichtung geeignet und erforderlich sind.

Grundsatz der Zweckbindung

Die Personendaten dürfen nur für den vorgegebenen Zweck verwendet werden.

⁴ Dabei handelt es sich um ein Individuum, also einen Menschen. Demgegenüber steht die juristische Person, also ein Unternehmen.

⁵ In der aktuell geltenden Fassung des DSG sind auch juristische Personen erfasst (Art. 1 Abs. 1 Bst c), was mit dem Nachtrag zum DSG geändert werden soll.

Grundsatz der Transparenz

Die Datenbearbeitung muss für die betroffene Person transparent sein.

Dieser Grundsatz heisst, dass eine betroffene Person aus den Umständen heraus mit einer Datenbeschaffung und dem Zweck der Datenbearbeitung rechnen musste oder dass sie entsprechend informiert bzw. aufgeklärt wird.⁶

Grundsatz der Datenqualität

Die Personendaten müssen aktuell, richtig und vollständig sein.

Grundsatz von Treu und Glauben

Es gelten der Vertrauensschutz und das Verbot widersprüchlichen Verhaltens und des Rechtsmissbrauchs.

Die Personendaten müssen mit organisatorischen und technischen Massnahmen vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten geschützt werden.

Beispiel:

Es muss geregelt sein, wer auf welche Klientendaten Zugriff hat und wie die Person diese bearbeiten darf (Leserecht, Bearbeitungsrecht).

Grundsatz der Verantwortung

Jede Person, die Personendaten bearbeitet, ist für die Einhaltung des Datenschutzes verantwortlich. Dies umfasst z.B. auch die Pflicht, sicherzustellen, dass nur diejenigen Personen Zugang zu den Personendaten haben, die dazu berechtigt sind.

1.4 Datenbearbeitung

Datenbearbeitung ist jeder Umgang mit Personendaten, insbesondere Beschaffung, Aufbewahrung, Verwendung, Bekanntgabe, Veränderung oder Vernichtung.

Die Datenbearbeitung ist zulässig, wenn:

- die betroffene Person eingewilligt hat;
- eine Rechtsgrundlage besteht **oder**
- die Datenbearbeitung zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist.

Bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen gelten erhöhte Anforderungen: Entweder muss das Gesetz (eine Verordnung allein reicht nicht aus) die Bearbeitung vorsehen **oder** die Bearbeitung muss zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich sein.

⁶ Basler Kommentar zum Datenschutz- und Öffentlichkeitsgesetz, Maurer-Lambrou/Steiner, Art. 4 N 16b.

Die für die sozialen Einrichtungen massgeblichen gesetzlichen Grundlagen richten sich nach den jeweiligen Aufgaben, für welche Daten bearbeitet werden.⁷

Die Einwilligung der betroffenen Person bzw. der zur Vertretung berechtigten Person (siehe dazu Ziff. 2.3.2) muss bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen ausdrücklich vorhanden sein. Es handelt sich beim Datenschutz um ein sogenanntes höchstpersönliches Recht, das insbesondere auch urteilsfähigen Minderjährigen zusteht.⁸ Die Einwilligung muss freiwillig sein, es dürfen keine Nachteile mit einer Verweigerung der Einwilligung verbunden sein. Zudem muss sie bezüglich des Verwendungszwecks genügend konkretisiert sein. Die betroffenen Personen müssen ausserdem über die Tragweite und Konsequenzen der Datenbearbeitung informiert sein und das Recht kennen, ihre Einwilligung zu widerrufen.

1.5 Rechte der betroffenen Person

1.5.1 Auskunft und Einsicht in eigene Daten

Den Klientinnen und Klienten ist auf Verlangen Auskunft und Einsicht in alle sie betreffenden Daten - insbesondere in die Klientendokumentation - zu gewähren. Dieser Anspruch gilt voraussetzungslos. Da es sich beim Auskunftsrecht um ein relatives, höchstpersönliches Recht handelt, können auch urteilsfähige Minderjährige und umfassend verbeiständete Personen das Auskunftsrecht selber, d.h. ohne Zustimmung der gesetzlichen Vertretung, ausüben.⁹ Auf Wunsch der betroffenen Person sollten ihr die Daten erläutert werden. Vom Auskunfts- und Einsichtsrecht ausgenommen sind persönliche Notizen der Mitarbeitenden der Einrichtungen, die lediglich als Gedankenstützen dienen (z.B. Agenda-Einträge, Planungsunterlagen, Gedächtnisstützen für Gespräche usw.).

Auskunft und Einsicht können abgelehnt, eingeschränkt oder mit Auflagen verbunden werden, wenn ein überwiegendes öffentliches oder schutzwürdiges privates Interesse Dritter entgegensteht. Als Auflage kann beispielsweise der Beizug einer Ärztin bzw. eines Arztes oder einer Vertrauensperson verlangt werden, falls eine entsprechende Schutzbedürftigkeit der betroffenen Person festgestellt wird.

Im Umfang der Gewährung der Einsicht wird den Klientinnen und Klienten schriftlich Auskunft (in Form von Aktenkopien) erteilt. Können sich die Einrichtung und die betroffene Person nicht über Umfang oder Form der Akteneinsicht einigen, ist die Aufsichtsbehörde zu konsultieren.

⁷ z.B. Art. 3 Abs. 2 des Gesetzes über die Pflegefinanzierung (sGS 331.2), Art. 13 Abs. 3 des Gesetzes über die soziale Sicherung und Integration von Menschen mit Behinderung (sGS 381.4).

⁸ Nach Art. 19c ZGB üben urteilsfähige handlungsunfähige Personen die Rechte, die ihnen um ihrer Persönlichkeit willen zustehen, selbstständig aus; vorbehalten bleiben Fälle, in welchen das Gesetz die Zustimmung des gesetzlichen Vertreters vorsieht.

⁹ Basler Kommentar zum Datenschutz- und Öffentlichkeitsgesetz, Gramigna/Maurer-Lambrou, Art. 8 N 7.

1.5.2 Berichtigung und Löschung

Die Klientinnen und Klienten haben Anspruch darauf, dass unrichtige Personendaten über sie berichtigt werden.

Kann weder die Richtigkeit noch die Unrichtigkeit von Klientendaten - insbesondere von solchen, die eine Wertung menschlichen Verhaltens enthalten - bewiesen werden, so können Klientinnen oder Klienten verlangen, dass ein entsprechender Vermerk mit ihrer eigenen Darstellung angebracht wird oder dass sie die Richtigkeit bestreiten (Bestreitungsvermerk).

1.5.3 Aufklärung über die Rechte

Alle Klientinnen und Klienten werden bei Eintritt in eine Einrichtung über ihre Rechte und Pflichten bezüglich Datenschutz aufgeklärt.

2 Häufige Fragen

2.1 Datenbearbeitung und Aktenführung

2.1.1 Welche Daten von betreuten Erwachsenen, Kindern und Jugendlichen darf eine Einrichtung bearbeiten?

Die Einrichtung darf Daten bearbeiten, wenn das Gesetz die Bearbeitung vorsieht, die Bearbeitung zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich ist oder wenn die betroffene Person im Einzelfall ausdrücklich sowie in Kenntnis von Zweck und Art der vorgesehenen Bearbeitung eingewilligt hat.

Dazu gehören insbesondere

- erforderliche Daten für den Betreuungsvertrag (z.B. Angaben zu Ansprüchen auf Sozialversicherungsleistungen);
- Angaben zur Finanzierung staatlicher Leistungen (z.B. Angaben im Zusammenhang mit dem webbasierten Abrechnungssystem CONNET, vgl. [Anleitung](#));
- erforderliche Informationen für die individuelle Förderplanung und Betreuung;
- Angaben zu gesundheitlichen Einschränkungen (z.B. ärztlich angeordnete Diät);
- usw.

Nicht dazu gehören in der Regel persönliche Korrespondenz oder biographische Angaben (soweit für die Betreuung nicht mehr relevant).

Zu beachten ist, dass die Datenschutzbestimmungen auch innerhalb einer Organisation bzw. Einrichtung eingehalten werden müssen. Das heisst, dass nicht alle Mitarbeitenden einer Einrichtung sämtliche Personendaten bearbeiten dürfen, beispielsweise durch beschränktes Zugriffsrecht oder eingeschränkte Einsicht. Jede Person darf nur diejenigen Daten bearbeiten, die sie für die eigene Aufgabenerfüllung benötigt oder wenn sie die Stellvertretung wahrnimmt.

2.1.2 Welche organisatorischen und technischen Massnahmen zur Sicherung der Daten hat die Einrichtung zu treffen?

Die Einrichtung hat organisatorische und technische Massnahmen zur Sicherung der Daten vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten zu treffen.

Die Sicherheitsmassnahmen betreffen allgemein den Zutritt zu Räumlichkeiten, den Zugang zu Rechnern und den Zugriff auf Dokumente.

Zu diesen Massnahmen zählen insbesondere:

- klare Regelung der Verantwortlichkeiten;
- Beschränkung der Zutritte zum Büro;
- Aufbewahrung von Akten mit Personendaten in abschliessbaren Schränken (Clear Desk);
- Klassifizierung von Dokumenten (geheim, vertraulich oder nicht klassifiziert) und Ablage im Laufwerk mit entsprechenden Zugriffsberechtigungen. Zur Klassifizierung ist die Verordnung über Informatiksicherheit anwendbar (sGS 142.21; Art. 7 ff). Diese ist zwingend für öffentliche Aufgabenträger und für Private, soweit ihnen Staatsaufgaben übertragen sind;
- Beschränkung von Zugriffsrechten bei elektronischen Laufwerken auf Personen, welche die Daten zur eigenen gesetzlichen Aufgabenerfüllung benötigen (z.B. nebst Hauptbearbeitung auch Stellvertretung und Sekretariat);
- Regelung des Umgangs mit Passwörtern;
- sicherer E-Mail-Versand;¹⁰
- allgemein sichere Kommunikation einschliesslich Legitimation/Identifikation der Empfängerin bzw. des Empfängers und Verhinderung eines Irrtums (falsche E-Mail-Adresse, falsche Fax-Nummer);
- Beachtung des Zugriffsrechts auch auf die Altaktenablage.

2.1.3 Was ist im Umgang mit sozialen Medien und Messenger-Diensten zu beachten?

Soziale Medien (Facebook, Google+, MySpace usw.) und Messenger-Dienste (z.B. WhatsApp) sind ungeeignet für den Umgang mit Personendaten aus sozialen Einrichtungen und unter deren Mitarbeitenden. Für ihre Nutzung entstehen zwar keine Kosten im Sinn von Geldbeträgen, gezahlt wird jedoch mit den Daten. Sowohl die Personendaten, die ausgetauscht werden, als auch die Metadaten (Verbindungsdauer, grobe geografische Herkunft der IP-Adresse, Verweildauer sowie Bewegungen auf der Seite usw.) werden von den Anbietenden gesammelt und ausgewertet. Zusätzlich können sich Übeltäter als sogenannte Freunde ausgeben und Nutzungsprofile in unredlicher Absicht verändert, ergänzt, kopiert oder für reale oder fiktive Personen erstellt werden, welche die sozialen Medien gar nicht nutzen.¹¹

¹⁰ Informationen zum sicheren E-Mail-Versand sind im Merkblatt der Fachstelle für Datenschutz enthalten: www.sg.ch → Sicherheit → Datenschutz → Themen → Kanton und Gemeinden.

¹¹ Weiterführende Informationen sind zu finden unter: www.edoeb.admin.ch → Datenschutz → Internet und Computer → Onlinedienste → Soziale Medien.

2.1.4 Was gilt nach Ablauf der Aufbewahrungspflicht?

Die Einrichtungen dürfen die Daten so lange aufbewahren, als sie diese für die Erfüllung ihrer gesetzlich vorgesehenen Aufgaben benötigen bzw. eine allfällige Aufbewahrungspflicht besteht. Nach Ablauf der Aufbewahrungspflicht müssen die Akten dem zuständigen Archiv angeboten werden.

2.1.5 Gibt es Kriterien, um bei der Erstellung oder Entgegennahme von Klientendaten¹² zu beurteilen, ob diese im betreffenden Klientendossier abgelegt und aufbewahrt werden müssen oder nicht?

Sämtliche Unterlagen, die geschäftsrelevant sind, d.h. für die Dokumentation und Nachvollziehbarkeit des Betreuungsverhältnisses wesentlich sind, müssen ins Klientendossier integriert, intern aufbewahrt und nach Ablauf der internen Aufbewahrungsfrist dem zuständigen Archiv angeboten werden.

2.1.6 Wie werden aufbewahrte Akten von anderen Stellen bei einem Gesuch um Einsicht in die eigenen Akten behandelt?¹³

Die betroffene Person hat das Recht auf Einsicht in sämtliche sie betreffende und durch die Stelle bearbeiteten Akten, unabhängig davon, ob es sich um eigene Akten oder solche von Dritten handelt. Einschränkungen der Einsicht können lediglich aufgrund überwiegender öffentlicher oder schutzwürdiger privater Interessen Dritter gemacht werden (vgl. dazu Ziff. 1.5.1).

2.1.7 Was bedeuten die Grundsätze der Verhältnismässigkeit und der Zweckbindung, erläutert anhand eines Beispiels?

Die Grundsätze der Verhältnismässigkeit und der Zweckbindung bedeuten, dass die Bearbeitung der Personendaten auf den Zweck bei deren Erhebung beschränkt ist. Wird beispielsweise beim Eintritt einer Person deren Gesundheitszustand abgefragt und müssen allfällige Arztzeugnisse eingereicht werden, dann heisst das für die:

- **Beschaffung:** Es dürfen nur diejenigen Angaben abgefragt werden, die für den Betreuungsauftrag relevant sind und nicht auf Vorrat weitere Daten erhoben werden. Neben dem Betreuungsvertrag kann sich der Zweck auch aus einer gesetzlichen Grundlage ergeben: Die Einrichtungen für Menschen mit Behinderung müssen für das Amt für Soziales beispielsweise jährlich den individuellen Betreuungsbedarf der betreuten Personen erheben, da die Leistungsabgeltung abgestuft und leistungsorientiert erfolgt.
- **Aufbewahrung:** Der Zugriff ist auf Mitarbeitende zu beschränken, die für die Aufgabenerfüllung auf Information angewiesen sind. Beispiel: Hauswirtschaftliche Angestellte müssen nur über angeordnete Diäten informiert sein, Pflegefachpersonal hingegen auch über die Medikation.
- **Bekanntgabe:** Wird beispielsweise für eine ambulante Behandlung eine Ärztin oder ein Arzt beigezogen, ist er auf die Informationen zum Gesundheitszustand angewiesen. Der Beistand, der mit der Vermögensverwaltung befasst ist, benötigt die Informationen in der Regel nicht.

¹² Beispielsweise Tagesjournale, Berichte, persönliche Korrespondenz.

¹³ Beispielsweise Arztzeugnis, medizinisches Gutachten oder Bericht einer Beratungsstelle.

2.1.8 Wie werden Kombinationen aus Initialen, Sozialversicherungsnummer und Geburtsdatum gewertet?

Wenn damit eine Person bestimmbar ist, handelt es sich um Personendaten, für die das Datenschutzgesetz gilt. Aufgrund bestimmter Merkmale oder aufgrund des Kontextes können Rückschlüsse auf bestimmte Personen gemacht werden. Es muss immer im Einzelfall beurteilt werden, ob es sich noch um Personendaten handelt oder nicht.

2.1.9 Welche Unterlagen dürfen die Einrichtungen in diesem Zusammenhang dem Amt für Soziales als Aufsichtsbehörde einreichen?

Das Amt für Soziales darf diejenigen Daten bearbeiten, die für die Aufsicht unentbehrlich sind oder für deren Bearbeitung eine Rechtsgrundlage besteht. Diese ergibt sich aus den jeweils anwendbaren Verordnungsbestimmungen.

Beispiele:

- Art. 8 der Verordnung über die soziale Sicherung und Integration von Menschen mit Behinderung (sGS 381.41)
- Art. 6 ff. der Verordnung über Kinder- und Jugendheime (sGS 912.4)
- Art. 3 der Verordnung über private Betagten- und Pflegeheime (sGS 381.18)

2.1.10 Was muss beachtet werden, wenn Dritte mit der Bearbeitung von Personendaten beauftragt werden?

Das Datenschutzgesetz lässt die Bearbeitung von Personendaten durch Dritte zu. Die Übertragung darf nicht durch Gesetz ausgeschlossen sein und die Dritten müssen Gewähr für die datenschutzrechtlich einwandfreie Bearbeitung bieten. Die Einrichtung muss die Einhaltung des Datenschutzes sicherstellen (durch Abschluss einer Vereinbarung, die auch den Datenschutz regelt). Die Einrichtung legt fest, dass die Personendaten nur so bearbeitet werden, wie sie dies selbst tun dürfte, dass die Personendaten nach den für das öffentliche Organ geltenden gesetzlichen Bestimmungen bearbeitet werden und vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten gesichert werden. Sie muss regelmässige Kontrollen durchführen und bei Nichteinhaltung die Übertragung rückgängig machen. Die Verantwortung für die Einhaltung der Datenschutzbestimmungen verbleibt bei der Einrichtung.

2.2 Datenbekanntgabe: Auskunft an und Einsicht durch Drittpersonen

2.2.1 Welche Vorkehrungen müssen bei telefonischen oder schriftlichen Anfragen getroffen werden, um den Datenschutz einzuhalten?

Beispiel:

Eine Person fragt telefonisch an, ob die Kostenübernahme für den Aufenthalt der betreffenden Person noch gewährleistet ist. Die anfragende Person bezeichnet sich als Beistandsperson. Darf auf diese Angabe betreffend Funktion (gesetzliche Vertretung) vertraut werden?

Ist die anfragende Person der sachbearbeitenden Person bekannt und hat sie sich bereits einmal ausgewiesen, sind keine weiteren Vorkehrungen bzw. Rückfragen notwendig.

Bei nicht bekannten Personen muss die Vertretungsbefugnis überprüft werden. Zu empfehlen ist, dass dies bei Aufnahme bzw. Eintritt einer verbeiständeten Person standardmässig erfolgt.

2.2.2 Welchen Personen dürfen Auskünfte erteilt und Einsicht gegeben werden?

Die Unterscheidung von Angehörigen bzw. nahestehenden Personen und weiteren Dritten ist datenschutzrechtlich nicht unmittelbar relevant. Die Grundsätze für die Bekanntgabe von besonders schützenswerten Personendaten sind die gleichen. Die Einrichtung darf Daten bekannt geben, wenn das Gesetz die Bekanntgabe vorsieht oder die betroffene Person eingewilligt hat.

Klientin bzw. Klient ist urteilsfähig

Familienangehörige (auch Ehepartner und Kinder) und weitere Bezugspersonen erhalten Auskünfte oder Einsicht:

- nur mit ausdrücklicher Einwilligung der Klientin oder des Klienten.

Weitere Dritte erhalten Auskünfte oder Einsicht:

- wenn das Gesetz entweder die Bekanntgabe vorsieht
- oder mit ausdrücklicher Einwilligung der Klientin oder des Klienten.

Klientin bzw. Klient ist nicht urteilsfähig¹⁴

Familienangehörige (auch Ehepartner und Kinder) und weitere Bezugspersonen erhalten Auskünfte oder Einsicht:

- mit Einwilligung der zur Vertretung der Klientin bzw. des Klienten berechtigten Person. Dies kann eine gesetzliche Vertretung, eine behördlich eingesetzte Vertretung oder eine mittels Vorsorgeauftrag von der Klientin oder dem Klienten bezeichnete Person sein, nicht jedoch die medizinische Vertretung (diese hat kein Recht zu bestimmen, ob Klientendaten jemandem bekannt gegeben werden dürfen, ausser es handle sich um die Weitergabe von Klientendaten im Rahmen der medizinischen Behandlung);
- je nach Urteilsfähigkeit bezüglich eines konkreten Ereignisses und nur mit Einwilligung der betroffenen Person.

Weitere Dritte erhalten Auskünfte oder Einsicht:

- wenn das Gesetz entweder die Bekanntgabe vorsieht;
- oder wie gegenüber Familienangehörigen und weiteren Bezugspersonen.

¹⁴ Ab welchem Alter Personen urteilsfähig sind, ist im Einzelfall zu beurteilen. Bezogen auf die Bearbeitung von Personendaten wird davon ausgegangen, dass dieses Alter bei ungefähr zwölf Jahren liegt.

Klientin bzw. Klient ist verstorben

Ist die Klientin oder der Klient verstorben, darf den Familienangehörigen sowie weiteren Bezugspersonen Auskunft erteilt und Einsicht in die Klientendaten gewährt werden, wenn die verstorbene Person zu Lebzeiten ihre Einwilligung dazu über ihren Tod hinaus erteilt hat. Gleichwohl empfiehlt sich eine konkrete Interessensabwägung je Einzelfall.

Andernfalls dürfen Familienangehörige sowie weitere Bezugspersonen, welche die verstorbene Person eng begleitet haben und somit über den Krankheitsverlauf grundsätzlich Bescheid wussten, in summarischer Weise über die Todesumstände informiert werden.

2.3 Recht der betroffenen Personen auf ihre persönlichen Daten

2.3.1 Darf eine betroffene Person die Vernichtung ihrer Akten verlangen?

Die betroffene Person hat Anspruch darauf, dass **widerrechtlich** bearbeitete Personendaten auf ihr Verlangen hin vernichtet werden. Widerrechtlich ist eine Datenbearbeitung dann, wenn weder eine Rechtsgrundlage besteht, noch die Datenbearbeitung für die Aufgabenerfüllung notwendig ist und keine Einwilligung der betroffenen Person vorliegt. Haben Personen bereits widerrechtlich bearbeitete Daten erhalten, muss die Einrichtung diese über die getroffenen Massnahmen (Vernichtung) informieren.

Bei **rechtmässig** bearbeiteten Personendaten besteht kein Recht auf Vernichtung der Akten.

2.3.2 Darf die betroffene Person die Berichtigung ihrer Akten verlangen?

Die betroffene Person darf die Berichtigung von offensichtlich unrichtigen Einzelangaben (z.B. Geburtsdatum, Schreibweise von Namen usw.) verlangen. Personendaten werten-der oder beschreibender Art, die von ihrer Natur her nicht bewiesen werden können, werden nicht berichtigt. Die betroffene Person kann jedoch verlangen, dass ein Bestreitungsvermerk oder eine Gegendarstellung angebracht wird.

2.4 Aufbewahrung und Archivierung von Klientendossiers

2.4.1 Aufbewahrungspflicht

Die Klientendokumentation wird nach Beendigung des Betreuungsverhältnisses während zehn Jahren durch das jeweilige Heim bzw. die stationäre Einrichtung aufbewahrt. Vorbehalten bleiben längere Aufbewahrungsfristen gestützt auf das Bundesrecht.

Die Aufbewahrungsfrist beginnt mit dem Abschluss der letzten Pflege- oder Betreuungshandlung zu laufen. Werden aufbewahrte Dokumente in eine Klientendokumentation für einen neuen Fall integriert, beginnt die Frist mit dem Austritt neu zu laufen.

Die Aufbewahrung kann in Papierform oder in elektronischer Form erfolgen.

2.4.2 Archivierung und Vernichtung

Nach Ablauf der in Ziff. 2.4.1 genannten Aufbewahrungsfrist wird die Klientendokumentation dem zuständigen Archiv zur Übernahme angeboten. Zur Klärung der archivischen Zuständigkeit können sich die Trägerschaften an das Staatsarchiv wenden. Bei Kinder- und Jugendheimen sowie bei Sonderschulen richtet sich die archivische Zuständigkeit nach den jeweiligen Archivierungskonzepten, die das Staatsarchiv im Jahr 2015 mit dem Amt für Soziales bzw. dem Amt für Volksschule abgeschlossen hat.

Bewertet das zuständige Archiv die Dokumentation als nicht archivwürdig, ist das Original vertraulich zu vernichten (z.B. durch Schreddern oder durch Verbrennen in der Kehrichtverbrennungsanlage unter Aufsicht) bzw. bei elektronischer Führung der Klientendokumentation durch endgültige Löschung der Daten (z.B. durch physische Vernichtung des Datenträgers). Ein Aufbewahrungsrecht der Einrichtung besteht nicht.

2.5 Informationssicherheit

2.5.1 Welche Daten dürfen über E-Mail-Korrespondenz zwischen der Einrichtung und Stellen der öffentlichen Verwaltung ausgetauscht werden?

Nach der Dienstanweisung über Einsatz und Verwendung von Informatikmitteln müssen kantonale Stellen bzw. kantonale Einrichtungen E-Mails mit besonders schützenswerten Personendaten, Persönlichkeitsprofilen oder Informationen über Angelegenheiten, die dem Amtsgeheimnis unterliegen, verschlüsselt versenden, wenn sie an Adressatinnen oder Adressaten ausserhalb des geschützten Kommunikationsnetzes KOMSG gerichtet sind. Dieser Standard gilt auch für nicht-kantonale Stellen. Besondere Bedeutung kommt auch dem Schutz gegen Irrtum zu.

2.5.2 Welche Alternativen zur Übermittlung von Personendaten sind zulässig? Gibt es Empfehlungen, die eine effiziente Abwicklung ermöglichen?

- Anonymisierung: Personendaten gelten dann als anonymisiert, wenn die Person nicht mehr bestimmbar ist. Unter «anonymisieren» versteht man jeglichen Vorgang, durch den die Zuordnung von Daten zu einer konkreten Person verhindert wird oder nur noch mit aussergewöhnlichem Aufwand möglich ist. Werden beispielsweise nur Initialen verwendet, kann häufig aufgrund des Kontextes auf die betroffene Person geschlossen werden;
- Verschlüsselung des E-Mail-Versands (SecureMail);
- passwortgeschützter ZIP-Ordner mit Personendaten;
- Nutzung einer sicheren Datenaustauschplattform des Kantons St.Gallen (ShareFile);
- für IVSE-anerkannte Einrichtungen: Datenübermittlung über das System CONNET;
- Postversand (insbesondere für sensible Daten zu empfehlen).

2.5.3 Ist die Sicherung und Aufbewahrung von besonders schützenswerten Personendaten in einer Cloud zulässig?

Der Einsatz von Cloud-Services ist nach dem Merkblatt «Cloud-spezifische Risiken und Massnahmen» von Privatim, der Konferenz der schweizerischen Datenschutzbeauftragten zu prüfen.¹⁵

3 Kontakt

Amt für Soziales
Spisergasse 41
9001 St.Gallen
T 058 229 33 18
info.diafso@sg.ch

Fachstelle für Datenschutz
Regierungsgebäude
9001 St.Gallen
T 058 229 14 14
datenschutz@sg.ch

4 Weiterführende Links

- [Datenschutzgesetz des Kantons St.Gallen](#)
- [Verordnung über die Informatiksicherheit des Kantons St.Gallen](#)
- [Bundesgesetz über den Datenschutz](#)
- [Verordnung zum Bundesgesetz über den Datenschutz](#)
- [Richtlinien zur Bearbeitung von Bewohnerdaten des Verbandes Heime und Institutionen Schweiz, CURAVIVA](#)
- [Datenschutz in der Sozialen Arbeit, eine Praxishilfe zum Umgang mit sensiblen Personendaten, Avenir Social, Bern 2013](#)
- [Weiterführende Informationen zu E-Health / Patientendossier](#)

¹⁵ www.privatim.ch → privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen».