1.2.2 Datenschutz-Konzept

Ziel und Zweck

Das Hauptziel dieses Konzepts ist, den Persönlichkeitsschutz der Bewohner*innen und Mitarbeiter*innen der Stiftung St. Beatus vor widerrechtlicher oder unverhältnismässiger Datenbearbeitung zu gewährleisten. Dieses Konzept soll als verbindliche Richtlinie alle für die Stiftung St. Beatus tätigen Personen unterstützen, in Eigenverantwortung datenschutzrechtlich einwandfrei zu handeln.

Geltungsbereich

Das vorliegende Datenschutz-Konzept der Stiftung St. Beatus bildet die verbindliche Grundlage für alle datenschutzrelevanten Massnahmen und Aktivitäten in der Stiftung St. Beatus. Es gilt für alle Organe und Mitarbeiter*innen der Stiftung, die im Rahmen ihrer Funktionen und Aufgaben Personendaten bearbeiten.
Es gilt ebenfalls für externe Personen und Unternehmen, sofern diese sich durch entsprechende schriftliche Vereinbarung zu dessen Einhaltung verpflichten.

Gesetzliche Grundlagen

Grundlage für dieses Datenschutzkonzept bilden das Datenschutzgesetz (KDSG; BSG 152.04; Stand am 01.11.2020) sowie die Datenschutzverordnung des Kantons Bern (DSV; Stand am 01.11.2020).

* * *

Grundsätze für das Bearbeiten von Personendaten und besonders schützenswerte Personendaten

Personendaten sind *Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen* (Art. 2 Abs. 1 KDSG). Jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten den betroffenen Personen zugeordnet werden können, gilt als **Datensammlung** (Art. 2 Abs. 2 KDSG).
Das **Bearbeiten** von Personendaten umfasst jeden Umgang mit Personendaten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten (Art. 2 Abs. 4 KDSG).

Bekanntgeben von Personendaten ist jedes Zugänglichmachen, wie etwa Einsicht gewähren, Auskunft geben, Weitergeben oder **Veröffentlichen** (Art. 2 Abs. 5 KDSG).
Beim Umgang mit „**besonders schützenswerten Personendaten**" ist besondere Vorsicht gefordert. Laut kantonalem Datenschutzgesetz (Art. 3 KDSG) sind das Angaben über:

- die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung sowie die ethnische Zugehörigkeit;
- den persönlichen Geheimbereich, insbesondere den **seelischen, geistigen oder körperlichen** (das heisst auch gesundheitlichen) **Zustand**;
- **Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung** (also z.B. alle Angaben, aus denen erschlossen werden kann, dass sich eine Person in einem Heim befindet);
- polizeiliche Ermittlungen, **Strafverfahren, Straftaten und die dafür verhängten Strafen und Massnahmen**.

Leitfragen für den Umgang mit Personendaten

Grundsätzlich ist immer zu fragen:

- Was wird
- mit welcher Zielsetzung
- in welchen Dokumenten erfasst,
- wie gesichert
- und wie lange aufbewahrt?

Was?

Grundsätzlich werden nur Daten erfasst, die für die professionelle Erfüllung des Auftrages notwendig sind. Im Gesetz heisst es: „Die Personendaten und die Art des Bearbeitens müssen für die Aufgabenerfüllung **geeignet und notwendig** sein."
Es dürfen **nicht mehr oder andere Daten** bearbeitet werden und es dürfen Daten **nicht länger** bearbeitet werden, als es die Aufgabenerfüllung erfordert (Art. 5 Abs. 3 KDSG).
Die notwendigen Informationen sollen, wenn möglich, direkt bei der **betroffenen Person beschafft** werden (Art. 9 Abs. 1 KDSG).
Zudem muss sichergestellt sein, dass die bearbeiteten Daten **richtig, vollständig und aktuell** sind (Art. 7 KDSG). Unrichtige und unvollständige Daten sind zu korrigieren oder zu vernichten.

Weshalb?

Vor der Erfassung von Personendaten ist deshalb immer zu fragen: Brauche ich – oder brauchen andere in der Institution – diese Daten wirklich, **um ihren Auftrag erfüllen zu können**?
Die Bearbeitung von Personendaten darf nur zu **bestimmten, kommunizierten oder erkennbaren Zwecken** erfolgen. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Erhebung oder Beschaffung angegeben wurde (Art. 5 Abs. 4 KDSG).

Besonders schützenswerte Personendaten dürfen überdies nur bearbeitet werden, wenn der Bearbeitungszweck zusätzlich in einem Gesetz oder einer Verordnung vorgesehen, die Erfüllung einer gesetzlichen Aufgabe dies zwingen erfordert oder die betroffene Person ausdrücklich zugestimmt hat (Art. 6 KDSG). Die gesetzliche Grundlage ist Art. 111 des Gesetzes über die sozialen Leistungsangebote vom 9. März 2021.

In welchen Dokumenten?

Wir unterscheiden grundsätzlich:

- Dokumente über Bewohner*innen
- Dokumente über Mitarbeiter*innen

Nach der **Art der Dokumente** unterschieden wir:

- schriftliches Arbeitsmaterial («Zettel» mit Infos oder Terminen, *Ausdrucke* z.B. von Mails, *Kopien* z.B. von Meldezetteln etc.)
- schriftliche Dokumente
    - über Bewohner*innen: Bewohner*innen-Ordner, Daten SocialWeb, Archiv und Archiv der Meldestelle
    - über Mitarbeiter*innen: Personaldossier, Archiv
- Verlaufsprotokolle
    - über Bewohner*innen: Vitalwerte (wenn erhoben), Journale im SocialWeb, Taschengeld-Blätter und Agenden
- Sitzungs-Protokolle
- Fotos/Videos

Wie gesichert und wie lange?

Nicht mehr benötigte Daten sind zu **vernichten** (Art. 19 Abs. 1 KSGD). Das bedeutet: **physisch zu zerstören oder elektronisch unwiederbringlich zu löschen**.

- **Schriftliches Arbeitsmaterial** («Zettel» mit Infos oder Terminen, Ausdrucke z.B. von Mails, Kopien z.B. von Meldezetteln etc.; auch schriftliche Dokumente, die noch nicht abgelegt sind) über Bewohner*innen ist *nur so lange bei den persönlichen Unterlagen des Mitarbeiters*der Mitarbeiterin zu behalten, wie er*sie die Angaben für seine*ihre aktuelle Arbeit braucht*. Die Informationen sind so bald wie möglich zu vernichten oder an die zuständige Bezugsperson (oder Meldestelle) weiterzuleiten, von dieser in geeigneter Weise zu verarbeiten und das Arbeitsmaterial abzulegen oder zu vernichten (schreddern oder klein zerreissen). Arbeitsmaterial **über Mitarbeiter*innen** ist umgehend im Personaldossier abzulegen oder zu vernichten.
  Für Arbeitsmaterial sind die jeweiligen Besitzer*innen verantwortlich. Es *darf nicht öffentlich zugänglich (nicht ausserhalb des Bürotraktes Berghaus bzw. den Team-Büros) aufbewahrt werden*.
  Schriftlichem Arbeitsmaterial ähnliche **elektronische Daten** dürfen *nur auf dem Desktop* des Mitarbeiters*der Mitarbeiterin abgespeichert werden; nicht auf einem auch für andere Mitarbeiter*innen zugänglichen Laufwerk. Sie sind zu löschen, sobald der*die Mitarbeiter*in sie nicht mehr für seine*ihre aktuelle Arbeit braucht. Dokumente von bleibendem Interesse sind wie (elektronische) „schriftliche Dokumente“ zu behandeln.

4

- **Schriftliche Dokumente**

  Über Bewohner*innen: Bewohner*innen-Ordner, Archiv und Archiv der Meldestelle.
  Bewohner*innen-Ordner sind laufend aktuell zu halten, unnötige bzw. unnötig gewordene Informationen/Dokumente sind zu vernichten. Nach Austritt des*der Bewohner*in ist der Bewohner*innen-Ordner innert dreier Monate zu archivieren.
  Sämtliche schriftlichen Unterlagen sind an einem nicht öffentlich zugänglichen Ort aufzubewahren (siehe schriftliches Arbeitsmaterial). Dafür sind die jeweiligen Bezugspersonen verantwortlich.
  Das Archiv verantwortet und führt der*die Leiter*in Administration. *Das Archiv ist unter Verschluss zu halten.* Zugang haben der*die IL, seine*ihre Stellvertreter*in sowie die Mitarbeiter*innen Administration. Archivierte Dokumente sind zehn Jahre nach Austritt des Bewohners*der Bewohnerin zu vernichten.
  Elektronische Dokumente über Bewohner*innen sind zwingend auf dem Laufwerk der Assistenz oder der Ateliers («SharePoint») bzw. im Socialweb abzuspeichern. Dokumente, die auf Papier (ausgedruckt) vorliegen, müssen nicht auch noch einmal elektronisch gespeichert werden bzw. bleiben. Werden sie elektronisch gespeichert, **muss die Struktur der elektronischen Ordner der**

Struktur der schriftlichen Ablage entsprechen[1]. Die elektronischen Ordner sind laufend aktuell zu halten, unnötige bzw. unnötig gewordene Informationen/Dokumente sind zu löschen. Die Verantwortung dafür liegt bei dem*der Mitarbeiter*in, der*die sie abgespeichert hat, bzw. der jeweils aktuellen Bezugsperson. Nach Austritt eines Bewohners*einer Bewohnerin ist der Bewohner*innen-Ordner innert dreier Monate in ein elektronisches Archiv auf dem Laufwerk der Administration zu verschieben. Archivierte Dokumente sind zehn Jahre nach Austritt des Bewohners*der Bewohnerin zu vernichten.

Über Mitarbeiter*innen: Personaldossier, Archiv. Die Personaldossiers sind laufend aktuell zu halten, unnötige bzw. unnötig gewordene Informationen/Dokumente sind zu vernichten[2]. Die Personaldossiers verantwortet und führt der*die Leiter*in Administration. *Die Personaldossiers sind unter Verschluss zu halten.* Zugang haben der*die IL, seine*ihre Stellvertreter*in sowie die Mitarbeiter*innen Administration. Nach Austritt eines Mitarbeiters*einer Mitarbeiterin sind die Personaldossiers innert dreier Monate dem Archiv zuzuführen und spätestens 20 Jahre nach Austritt des Mitarbeiter*/der Mitarbeiterin zu vernichten[3].

Bewerbungsunterlagen sind während eines laufenden Bewerbungsprozesses so aufzubewahren, dass nur Personen Zugriff haben, die mit der Besetzung der Stelle zu tun haben. Nach Anstellung der Person müssen die Daten ins Personaldossier überführt werden. Unterlagen von Bewerber*innen, denen eine Absage erteilt wurde, sind ihm*ihr zurückzusenden. Will der*die Bewerber*in ihre Unterlagen nicht zurücknehmen, sind die Daten zu vernichten.

- **Elektronische Dokumente** über Mitarbeiter*innen sind zwingend auf dem Laufwerk der Administration oder der Leitung abzuspeichern. Nach Austritt eines Mitarbeiters*einer Mitarbeiterin sind ihn*sie betreffende Dateien in ein elektronisches Archiv auf dem Laufwerk der Administration zu verschieben und spätestens 20 Jahre nach Austritt des Mitarbeiters*der Mitarbeiterin zu löschen.

- **Verlaufsprotokolle**.

  Bei uns: **Vitalwerte (wenn erhoben), Taschengeld-Blätter und Agenden.** Sämtliche Einträge über namentlich genannte oder aufgrund der Darstellung identifizierbare Personen sind - **mit Datum**

[1] So sind z.B. die elektronischen Bewohner*innen-Ordner in Unter-Ordner zu gliedern, die den Registern der Bewohner*innen-Ordner in Papier entsprechen und elektronische Dokumente entsprechend abzulegen.
[2] In der Regel sind das alle Unterlagen, die für die Erstellung und Begründung eines Arbeitszeugnisses nicht mehr benötigt werden, darunter insbesondere Notizen über Führungsgespräche, die älter sind als zwei Jahre, gegebenenfalls auch graphologische, psychologische oder medizinische Gutachten sowie Persönlichkeitstests.
[3] Bewerbungsunterlagen, wie z.B. Lebenslauf, frühere Arbeitszeugnisse, Ausbildungsdiplome, Arbeitsproben, Fotos und ähnliche Akten, die den Angestellten gehören und an denen der Arbeitgeber kein berechtigtes Interesse mehr hat, müssen spätestens bei Beendigung des Arbeitsverhältnisses zurückgegeben werden.

versehen - zu visieren und nach spätestens zwölf Monaten abzulegen, Agenden sind zu vernichten. Journaleinträge im SocialWeb werden nach zehn Jahren gelöscht.

- **Sitzungs-Protokolle**.

  Sitzungs-Protokolle sind grundsätzlich nur den Mitarbeiter*innen zugänglich zu machen, die davon unmittelbar betroffen sind (GMS, ATS, ASS und Rat: alle Mitarbeiter*innen). Verteilte Kopien sind wie schriftliches Arbeitsmaterial zu handhaben.
  Sitzungs-Protokolle sind spätestens nach zehn Jahren zu vernichten bzw. zu löschen.

- **SocialWeb.**

  Dossiers über Bewohner*innen sowie Mitarbeiter*innen im SocialWeb werden bei Austritt derselben auf «inaktiv» gesetzt und sind dann nur noch Mitarbeiter*innen mit Administratorenrechten zugänglich (IL, Mitarbeiter*innen Administration). Zehn Jahre nach Austritt werden sie durch SocialWeb gelöscht. Verantwortlich: Leiter*in Administration.

- **Fotos/Videos.**

  Mitarbeiter*innen der Stiftung veröffentlichen grundsätzlich keine Fotos/Videos, auf denen Bewohner*innen und/oder Mitarbeiter*innen zu erkennen sind. Veröffentlichung meint dabei jede Veröffentlichung in Print, aber auch auf sozialen Plattformen wie Facebook, Instagram oder das Versenden an Dritte über Dienste wie WhatsApp oder Snapchat. Bewohner*innen sind entsprechend zu sensibilisieren.

  Wer Fotos/Videos für den internen Gebrauch anfertigt (z.B. von Ausflügen, Lagern etc.) speichert sie umgehend auf Datenaustausch oder dem Foto-Ordner der Wohngruppe bzw. auf dem Atelier-Laufwerk – und löscht sie von seinem privaten Gerät. Spätestens nach zehn Jahren werden sie gelöscht. Verantwortlich dafür ist der*die IL.
  Vor der Veröffentlichung von Fotos/Videos durch die Stiftung ist in jedem Fall schriftlich die Zustimmung des*der Urheber*in sowie die ausdrückliche Zustimmung der erkennbar abgebildeten Person(en) einzuholen. Die Zustimmung der betroffenen Person(en) muss freiwillig, ausdrücklich und nach vorgängiger Aufklärung über den Zweck und die Verwendung der Aufnahme(n) erfolgen und vorzugsweise schriftlich aufbewahrt werden.

* * *

Datensicherheit

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

- **Organisatorische Massnahmen.**
  Der Zugang zu Personendaten besteht bei der Stiftung St. Beatus nach dem Grundsatz «so viel wie nötig, so wenig wie möglich».
- **Technische Massnahmen.**
  Der Schutz elektronisch bearbeiteter Daten wird insbesondere durch Verschlüsselung, den Einsatz von Firewalls, Virenschutzprogrammen etc. und die Protokollierung von Zugriffen gewährleistet. Die Datenbearbeitungssysteme sind so eingerichtet, dass jede Datenbearbeitung (z.B. Zugriff, Einsichtnahme, Mutation) automatisch festgehalten wird. Damit kann jederzeit festgestellt werden, ob die Daten für diejenigen Zwecke bearbeitet worden sind, für die sie erhoben wurden.
  Durch ein Zugangs- und Berechtigungsmanagement wird verhindert, dass unbefugte Personen Zugang zu Datenbeständen haben oder diese verändern, entwenden, zerstören etc. können.

* * *

Schweigepflicht

Alle Mitarbeiter*innen der Stiftung St. Beatus werden darauf hingewiesen, dass

- sie der beruflichen Schweigepflicht und ggf. weiteren gesetzlichen Geheimhaltungspflichten unterliegen;
- die Geheimhaltungspflichten auch nach Austritt aus der Stiftung St. Beatus weiterbestehen;
- eine Verletzung von Geheimhaltungspflichten oder datenschutzrechtlichen Sorgfaltspflichten zu arbeitsrechtlichen, straf- und zivilrechtlichen Konsequenzen führen kann.

Die berufliche Schweigepflicht gilt nicht der betroffenen Person gegenüber. Sie gilt aber gegenüber allen „Dritten“, d.h. **auch gegenüber Angehörigen**. Sie umfasst insbesondere die „besonders schützenswerten Personendaten“ (siehe oben), den Inhalt der Dossiers und anderer interner Dokumente. Auskünfte über solche Daten erteilen ausschliesslich die jeweils zuständigen Bezugspersonen oder der*die IL bzw. seine*ihre Stellvertreter*in – nachdem sie sich davon überzeugt haben, dass die anfragende Person informationsberechtigt ist. *Auch innerhalb des Heimes*

*ist der Kreis derer, die Zugang zu Personendaten haben, auf diejenigen Mitarbeiter*innen zu beschränken, für deren Arbeit die Daten notwendig sind.*

Die **Weitergabe von Personendaten an Dritte**

- muss sich auf eine **gesetzliche Grundlage** stützen (insbesondere Melde- und Anzeige-Pflichten bzw. –Rechte und Pflichten zur Auskunftserteilung),
- von der betroffenen Person **im Einzelfall bewilligt** sein,
- zur **Abwendung einer unmittelbar drohenden Gefahr für Leib und Leben** notwendig sein
- oder im Rahmen der **Amtshilfe** erfolgen.

(**Amtshilfe** heisst: Es liegt eine Anfrage einer Behörde vor, die Daten werden zur Aufgabenerfüllung benötigt, die Aufgabe kann anders nicht erfüllt werden und der Zweck, zu dem die Daten ursprünglich erfasst wurden, ist der gegenwärtigen Aufgabe ähnlich.)

Sperrung der Datenbekanntgabe

Jede*r Bewohner*in und jede*r Mitarbeiter*in kann die Bekanntgabe seiner*ihrer Daten sperren lassen, wenn er*sie ein schutzwürdiges Interesse nachweist. Die Bekanntgabe ist trotz Sperre zulässig, 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. Geht ein entsprechendes Gesuch ein, wird dies an den*die Institutionsleiter*in zur Beantwortung weitergegeben.

*** * ***

Auskunfts- und Einsichtsrecht

Jede*r Bewohner*in und jede*r Mitarbeiter*in hat das Recht über Erhebung, Herkunft, Inhalt, Zweck, Kategorie und Rechtsgrundlage der Bearbeitung seiner*ihrer Daten informiert zu werden sowie Einsicht in das über sie*ihn geführte Dossier zu verlangen (SocialWeb, Bewohner*innen-Ordner, Personaldossier, Archiv).

Die Auskunft bzw. Einsicht verlangende Person muss sich über ihre Identität ausweisen. Ihr ist in allgemeinverständlicher Weise, schriftlich und kostenlos Auskunft bzw. Einsicht zu erteilen. Die Auskunft bzw. Einsicht gewährt ausschliesslich die zuständige Bezugsperson (bei Bewohner*innen) oder die Institutionsleitung. Die Einsicht erfolgt bei Bewohner*innen in der Regel begleitet. Der*die Bewohner*in, der*die Mitarbeiter*in darf sich Notizen machen (keine Fotos); Ausdrucke oder Kopien werden nicht abgegeben.

Die Stiftung St. Beatus kann die Auskunft bzw. Einsicht ausnahmsweise einschränken, aufschieben oder verweigern, wenn wichtige und überwiegende öffentliche Interessen oder besonders schützenswerte Interessen von Dritten entgegenstehen.
Besteht das Risiko, dass die betroffene Person mit der Auskunftserteilung oder Einsichtnahme einer zu hohen Belastung ausgesetzt werden könnte, kann sie eine andere Person bestimmen, der an ihrer Stelle Auskunft erteilt bzw. Einsicht gewährt wird.

Recht auf Berichtigung

Jede*r Bewohner*in und jede*r Mitarbeiter*in kann verlangen, dass **unrichtige oder nicht notwendige Personendaten** über ihn*sie berichtigt oder vernichtet werden. Wenn die Richtigkeit der Daten strittig ist, muss eine angemessene Gegendarstellung aufgenommen werden. Überdies hat jede*r Bewohner*in und jede*r Mitarbeiter*in Anspruch darauf, dass Personendaten, die widerrechtlich bearbeitet worden sind, vernichtet und/oder die Folgen der Widerrechtlichkeit beseitigt werden.

Orientierung der Betroffenen

Bewohner*innen und Mitarbeiter*innen werde beim Eintritt über ihre datenschutzrechtlichen Rechte und Pflichten informiert. Der*Die Institutionsleiter*in orientiert sie angemessen über die Beschaffung der sie betreffenden Personendaten.

* * *

<u>Grundsätze im Umgang mit elektronischen Daten</u>

Bei der Arbeit mit internen Daten gilt grundsätzlich:

- ✓ <u>Individuelle Passwörter nicht weitergeben</u>, insbesondere nicht an Personen anderer Teams oder Dritte (oder wenn, dann danach das Passwort ändern). Beruflich verwendete Passwörter sollten nicht für private Accounts verwendet werden. Im Homeoffice oder auf privaten Computern dienstlich genutzte Passwörter <u>nicht (im Browser) abspeichern, sondern jedes Mal neu eingeben</u>.
- ✓ <u>PC sperren oder ausloggen, wenn ihr den Raum verlasst</u> (und andere Mitarbeiter*innen, Bewohner*innen oder Dritte Zugang zu dem Raum haben).

Bei jedem Zugriff auf elektronische Dokumente, die potenziell besonders schützenswerte Personendaten enthalten (**E-Mails, SocialWeb**) ist auf Folgendes zu achten:

- ✓ Niemals Dritten Zugang zu oder Einblick in solche Dokumente gewähren,

- ✓ in geschützter Atmosphäre arbeiten - sicherstellen, dass niemand «über die Schulter schauen» kann.
- ✓ Auch im Homeoffice gilt: Bildschirm beim Verlassen des Arbeitsplatzes sperren.

Beim Gebrauch von Geräten bzw. Profilen, auf die auch andere Personen Zugang haben keine Passwörter abspeichern. Auch sonstige zu beruflichen Zwecken bearbeitete Personendaten dürfen nicht auf privaten Geräten gespeichert werden. Sollte über das Handy Zugriff auf E-Mails mit Personendaten erfolgen bzw. werden die E-Mails auf dem Handy gespeichert, darf kein Backup davon auf einer privaten Cloud gespeichert werden.

In E-Mails sind grundsätzlich nur Vornamen und die Initialen des Nachnamens zu verwenden (z.B. «Petra M.»). Grundsätzlich sind möglichst wenig Personendaten per E-Mail zu übermitteln. Sie dürfen keine sensiblen Informationen oder Angaben über Passwörter und andere Zugangsdaten enthalten. Besonders schützenswerten Daten dürfen grundsätzlich nach aussen nur **verschlüsselt** per E-Mail übermittelt werden, sofern die betroffene Person keine gegenteilige, schriftliche Erklärung abgegeben hat. Hierfür ist jeweils die HIN-Adresse zu verwenden.

E-Mails mit personenbezogenen Daten sind wie elektronische schriftliche Dokumente zu behandeln: Unnötige bzw. unnötig gewordene Informationen/Dokumente sind zu löschen. Das Profil austretender Mitarbeiter*innen wird spätestens nach einem halben Jahr gelöscht, inklusive aller darin gespeicherten Daten; das betrifft auch alle E-Mails.

* * *

Verantwortlichkeiten

Der **Stiftungsrat** ist auf strategischer Ebene für die Gewährleistung des Datenschutzes bei der Stiftung St. Beatus verantwortlich.

- ➢ Er nimmt den Datenschutz als relevantes Thema in sein Risikomanagement-System auf und beurteilt die entsprechenden Risiken in strategisch stufengerechter Weise.
- ➢ Er erlässt das vorliegende Datenschutzkonzept und überprüft dieses regelmässig.

Datenschutzbeauftragte der Stiftung ist Chantal Lutz (Ressort Rechtsgeschäfte im Stiftungsrat). Sie ist auch für das Interne Kontroll-System (IKS) Informatik-Systeme verantwortlich.

Der*Die **Institutionsleiter*in** ist für die Umsetzung des Konzepts und für die Einhaltung der datenschutzrechtlichen Vorgaben im Rahmen aller Datenbearbeitungen auf operativer Ebene letztverantwortlich. Zudem sorgt er*sie in geeigneter Weise dafür, dass alle Mitarbeiter*innen regelmässig für die Belange des Datenschutzes sensibilisiert und über die Vorgaben dieses Konzepts und deren Anwendung im beruflichen Alltag informiert werden.

- Er*Sie nimmt betriebsintern die Aufgaben gemäss der Gesetzgebung und dem Pflichtenheft wahr.
- Er*Sie ist nach innen und aussen die Ansprechperson für alle Fragen bezüglich des Datenschutzes.
- Er*Sie prüft die Rechtmässigkeit der Datenbearbeitung bei der Stiftung St. Beatus.
- Er*Sie verfügt über ein Weisungsrecht, soweit dies für die Einhaltung der Gesetzgebung und die Umsetzung dieses Konzepts erforderlich ist.
- Er*Sie erstattet gegebenenfalls Meldungen an die Datenschutzbeauftragten des Kantons.
- Er*Sie berichtet dem Stiftungsrat regelmässig über die Datenbearbeitung in der Stiftung St. Beatus, weist dabei auf erkannte Risiken hin und gibt Empfehlungen für mögliche Verbesserungen ab. Über besondere Vorkommnisse von grösserer Tragweite orientiert er*sie den Stiftungsrat unverzüglich.
- Er*sie steht dem Stiftungsrat, dem*der Leiter*in Administration, den Mitarbeiter*innen sowie Bewohner*innen bei datenschutzrechtlichen Fragen beratend zur Verfügung.

Der*die **Leiter*in Administration** ist für die sorgfältige und datenschutzkonforme Bearbeitung der Personendaten der Mitarbeiter*innen im Rahmen der Personalarbeit verantwortlich.

11

Alle **Mitarbeiter*innen** der Stiftung St. Beatus, welche Personendaten bearbeiten, tragen dem Datenschutz eigenverantwortlich Rechnung und handeln dabei insbesondere gemäss dem vorliegenden Konzept und den Weisungen des Institutionsleiters*der Institutionsleiterin. Sie wenden sich bei Datenschutzfragen und Unsicherheiten an den*die Institutionsleiter*in.