F 4.7 Datenschutz

Geltungsbereich: Gesamte Einrichtung

1. Einführung

Maßnahmen des Datenschutzes und der Datensicherheit dienen dazu, Kunden und Mitarbeiter davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt werden. Für Einrichtungen in der evangelischen Trägerschaft gilt insbesondere das Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD).Spezialgesetzliche Regelungen zum Datenschutz finden sich beispielsweise im Sozialgesetzbuch (SBG) im Strafgesetzbuch (STGB), im Telekommunikations- und Telemediengesetz (TKM, TMG)

2. Ziele

- Die rechtlichen und kirchlichen Datenschutzbestimmungen werden eingehalten.
- Ein sachgerechter Umgang mit persönlichen Daten von Kunden/ Bewohnern und Mitarbeitern ist sichergestellt.
- Das Recht auf Gewährleistung der informationellen Selbstbestimmung wird berücksichtigt.

3. Qualitätskriterien

- Das **schriftliche** Datenschutzkonzept beinhaltet mindestens folgende Kriterien:

- Datenschutzbeauftragte ist ernannt
- Beschreibung der IT Sicherheitsmaßnahmen und Dokumentation der Umsetzung der technischen/ organisatorischen Anforderungen
- einholen von Einwilligungen vor/ zur Veröffentlichung und weiteren Verwendung von Fotos und Namen
- Regelungen zum Umgang mit dem Internet und E- Mails für Mitarbeiter
- Regelungen zum Umgang mit Briefen und Post der Kunden
- Regelung zur Überprüfung der Einhaltung des Datenschutzes

- Die Mitarbeiter werden regelmäßig zum Thema Datenschutz und Verschwiegenheitspflicht geschult.

- Verpflichtungserklärung auf das Datengeheimnis liegen allen Mitarbeitern unterschrieben vor.

- Vereinbarungen zur Auftragsdatenverarbeitung mit Auftragsdatenverarbeitern (externe Dienstleister) liegen vor.

- Es gilt das Gebot der Datenvermeidung und Sparsamkeit.

- die Impressumspflichten auf den eigenen Internetseiten werden eingehalten

Datenschutzkonzept, nach Einführung der DSGVO vom 25.05.2018

Ziele

Ziel des Datenschutzes ist die Gewährleistung des allgemeinen Persönlichkeitsrechts des Einzelnen bei der Verarbeitung personenbezogener Daten. Es gilt der Schutz des Rechts auf informationelle Selbstbestimmung. Personenbezogene Daten von Bewohnern und Mitarbeitern dürfen nicht beliebig erhoben, verarbeitet oder genutzt werden.
Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Rechtsvorschrift dies erlaubt oder wenn der Betroffene hierzu wirksam eingewilligt hat. Gesundheitsdaten der Bewohner gelten als besondere Arten personenbezogener Daten und unterliegen besonders restriktiven Schutzregelungen. Aufgrund dieser besonders sensiblen Gesundheitsdaten fällt dem Datenschutz in unserer Einrichtung ein hoher Stellenwert zu.
Zur Sicherstellung des Datenschutzes sind festzulegende betriebliche Schutzmaßnahmen erforderlich, die einen unzulässigen Umgang mit personenbezogener Daten möglichst auszuschließen. Maßnahmen zur Gewährleistung von Datenschutz müssen neben technische Sicherheitsmaßnahmen wie Zugriffsrechte oder Regelungen zu Passworten auch organisatorische Festlegungen wie Unterweisungen und Qualifizierungsmaßnahmen für die Beschäftigten umfassen. Ohne das notwendige Wissen und Verständnis bei den betroffenen Mitarbeitern und ihrem Vorgesetzten kann Datenschutz nicht wirksam umgesetzt werden.

Rechtsgrundlagen

Für unsere Einrichtung ergeben sich die wesentlichen Rechtsvorschriften aus der Schweigepflicht nach § 203 StGB, dem Datenschutzgesetz sowie diversen bereichsspezifischen Datenschutzregelungen.
Unsere Einrichtung unterliegt dem Datenschutzgesetz der evangelischen Kirche in Deutschland (DSG-EKD)
Weitere wesentliche Rechtsgrundlagen zum Datenschutz sind:

- § 203 StGB: Schweigepflicht für Pflegekräfte (als Angehörige eines Heilberufs mit staatlich geregelter Berufsausbildung)
- Sozialgesetzbuch, 11. Buch (SGB XI – Soziale Pflegeversicherung), dabei besonders:
  - Neuntes Kapitel: Datenschutz und Statistik (§§ 93 – 109)
- Telemediengesetz (TMG)
- Telekommunikationsgesetz (TKG)
- Kunsturhebergesetz (KunstUrhG)

Eine Übermittlung von Bewohner- oder Mitarbeiterdaten an externe Stellen findet aufgrund der Schweigepflicht nach § 203 StGB nur statt,

- wenn dies für die Behandlung des Bewohners, das Arbeitsverhältnis des Mitarbeiters erforderlich ist und der Bewohner/ der Mitarbeiter nicht widersprochen hat oder
- wenn eine gesetzliche Offenbarungsbefugnis vorliegt oder
- wenn der Bewohner/ der Mitarbeiter eingewilligt hat.

Alle wesentlichen Rechtsvorschriften können in der Verwaltung im Ordner „Datenschutz“ eingesehen werden.

Verantwortliche Personen

Rechtlich verantwortlich für den Datenschutz ist die Geschäftsführung. Die Umsetzung des Datenschutzes funktioniert aber nur dann, wenn jeder Mitarbeiter und jeder Vorgesetzte in seinem Bereich seinen Beitrag leistet und die festgelegten Regelungen zum Datenschutz einhält.
Eine wichtige Aufgabe kommt auch dem Datenschutzbeauftragten zu. Er wirkt auf die Einhaltung der Bestimmungen für den Datenschutz hin und unterstützt die Geschäftsführung bei der Sicherstellung des in ihrer Verantwortung liegenden Datenschutzes. Zu seinen Aufgaben gehört die Überwachung der ordnungsmäßigen Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, und die Unterweisung der bei der

Verarbeitung personenbezogener Daten tätigen Personen hinsichtlich der Bestimmungen über den Datenschutz.
Der Datenschutzbeauftragte überwacht die Umsetzung des Datenschutzes durch regelmäßig stattfindende Datenschutzaudits. Er führt mindestens einmal jährlich Unterweisungen zum Datenschutz durch.
Der Datenschutzbeauftragte ist der Geschäftsführung direkt unterstellt und ist im Rahmen seiner Aufgaben weisungsfrei. Jeder Betroffene – Bewohner wie Mitarbeiter – kann sich bei Fragen oder vermuteten Datenschutzverstößen an ihn wenden.
Die technische Umsetzung des Datenschutzes und der IT-Sicherheit wird durch die Firma XY geleistet. Für diese Dienstleistung ist mit dem externen Auftragnehmer ein entsprechender Vertrag abgeschlossen.

Verpflichtung zum Datenschutz (§ 203 StGB Gültig vom 22.09.2017)
Allen Mitarbeitern der Einrichtung ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Sie haben insbesondere auch die Schweigepflicht hinsichtlich der Bewohnerdaten zu gewährleisten. Alle Mitarbeiter werden auf die Einhaltung der Bestimmungen des Datenschutzes und der Schweigepflicht nach § 203 StGB schriftlich verpflichtet. Dies wird in der Regel im Rahmen der Einstellung vollzogen. Die Verpflichtungserklärung wird eingeholt mit den Einwilligungen lt. DSGVO vom 25.05.2018 und in die Personalakte aufgenommen.

Technische Maßnahmen zur Umsetzung des Datenschutzes im IT-Bereich
Der Datenschutz wird in der Einrichtung soweit wie möglich durch präventiv wirkende technische Sicherheitsmaßnahmen gewährleistet, die eine unzulässige Verarbeitung und Nutzung personenbezogener Daten weitgehend auszuschließen.
Dazu werden die IT-Systeme und die gesamte IT-Infrastruktur durch Firewalls, Virenschutzsoftware und ein differenziertes Berechtigungskonzept abgesichert. Jeder Benutzer erhält eine persönliche, passwortgestützte Benutzererkennung und Zugriffsberechtigungen nur in dem Umfang, wie sie zur Durchführung der eigenen Arbeitsaufgaben erforderlich sind. Die Server und zentrale IT-Geräte werden geschützt, die erforderlichen räumlichen Voraussetzungen zur Umsetzung des Datenschutzes sind geschaffen. Die Daten werden regelmäßig zentral gesichert. Personenbezogene Daten werden an externe Stellen – sofern zulässig – nur in sicherer verschlüsselter Form übermittelt.

Datenschutzinformationen
Die Rechtsvorschriften, Datenschutzrichtlinien, Merk- und Formblätter zum Datenschutz stehen allen Mitarbeitern zur Einsicht in der Verwaltung zur Verfügung.
Die inhaltliche Verantwortung für diese Informationen liegt beim Datenschutzbeauftragten. Er pflegt die Inhalte und ergänzt diese um aktuelle Mitteilungen zum Datenschutz.

Technisch-organisatorische Schutzmaßnahmen
Zutrittskontrolle
- Büroräume sind beim Verlassen zu verschließen. Dies gilt insbesondere für Dienstzimmer in den Wohnbereichen. Akten, Unterlagen oder Papiere mit Bewohner- oder Mitarbeiterdaten sind so aufzubewahren, dass Unbefugten kein Zugriff ermöglicht wird.
- Beim Verlassen des Dienstzimmers müssen Bewohnerunterlagen und Bewohnerdaten gegen den Zugriff durch Unbefugte in geeigneter Weise gesichert werden. Bei Abwesenheit sind Dienstzimmer abzuschließen. Aushänge im Dienstzimmer mit personenbezogen Daten von Mitarbeitern und Bewohnern sind zu unterlassen. (ggf. in Dokumentenmappe zu sammeln und an sicherem Ort aufzubewahren- Zugriff für Dritte ist nicht zulässig.)
- In Bereichen mit Publikumsverkehr sind Monitore, Drucker und Faxgeräte so aufzustellen, dass das Risiko der Einsichtnahme Dritter ausgeschlossen wird.

– Archivräume sind verschlossen zu halten, wenn sich kein zuständiger Mitarbeiter darin aufhält. Zugang zu Archivräumen erhalten nur dafür zuständige Mitarbeiter der Heimverwaltung durch entsprechende Schlüsselvergabe.

Zugangskontrolle
– Arbeitsplatzrechner in Arbeitsräumen, die beim Verlassen nicht regelmäßig abgeschlossen werden, sind zum Schutz vor unbefugten Personen mit einem passwortgeschützten Bildschirmschoner ausgestattet, der nach ***10-30*** Minuten Wartezeit automatisch aktiviert wird. Dieser darf vom Benutzer nicht deaktiviert werden.

Zugriffskontrolle
– Beim Verlassen eines Arbeitsplatzrechners muss sich der Benutzer am Gerät abmelden, sofern nicht durch Verschluss des Raumes sichergestellt werden kann, dass kein anderer Benutzer Zugriff auf das Gerät nehmen kann. Bei kurzfristiger Abwesenheit kann er anstelle der Abmeldung auch den Bildschirm sperren (Windows-Taste + „L“).

Weitergabekontrolle
– Sollen personenbezogene Daten auf elektronischem Wege an einen Dritten außerhalb der Einrichtung übermittelt werden, dann darf dies nur im Rahmen eines freigegebenen IT-Verfahrens, das eine sichere Übertragung der Daten gewährleistet, erfolgen. Ohne Einwilligung der Betroffenen dürfen per Email keine personenbezogene Daten an externe Empfänger verschickt werden.
– Ausdrucke mit personenbezogenen Daten sind umgehend aus dem Drucker zu entfernen.

Eingabekontrolle
– Es muss nachträglich überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Deshalb werden die Dateneingaben, insbesondere bei Personenbezogenen Daten protokolliert.

Auftragskontrolle
– Personenbezogene Daten, welche im Auftrag verarbeitet werden, sollen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Deshalb haben wir mit Externen entsprechende Verträge geschlossen und überprüfen in Abständen die Einhaltung der Vorgaben.

Verfügbarkeitskontrolle
– Unsere Daten sind gegen zufällige Zerstörung oder Verlust geschützt. Der Schutz erfolgt durch tägliche und monatliche Datensicherungen, eine unterbrechungsfreie Stromversorgung bei Servern sowie durch festgelegte Notfallmaßnahmen in unserem IT - Notfallkonzept

Datentrennung
– Personenbezogene Daten, die wir zu unterschiedlichen Zwecken erheben werden getrennt verarbeitet. Dies wird durch technische oder logische Trennung von Datenbeständen sichergestellt.

Besonderheiten beim Umgang mit Bewohnerdaten

- Für die Erhebung, Verarbeitung und Nutzung von Bewohnerdaten gelten besonders restriktive Zulässigkeitsvoraussetzungen. Dabei sind insbesondere die Regelungen in § 39 er Datenschutzgesetzverordnung (DSGVO) der EKD zu beachten.
- Weiterhin gilt für Bewohnerdaten in elektronsicher wie konventioneller Form eine besondere Schweigepflicht nach § 203 Strafgesetzbuch. Verstöße können mit Freiheitsstrafe bis zu einem Jahr (in besonders schweren Fällen bis zu zwei Jahren) oder Geldstrafe geahndet werden. Die Schweigepflicht gilt grundsätzlich auch gegenüber den Mitarbeitern außerhalb des Wohnbereichs, in dem Sie tätig sind.
- Einwilligungen von Bewohnern bzw. Entbindungen von der Schweigepflicht sind in schriftlicher Form einzuholen.

Führung der Pflegedokumentation

- Die Führung einer Pflegedokumentation ist eine im Rahmen einer ordnungsgemäßen Pflege erforderliche Leistung (gemäß § 3 der Rahmenberufsordnung für beruflich Pflegende). Verantwortlich für die Ordnungsgemäßheit der Dokumentation und die Wahrung der Schweigepflicht sind die Pflegedienstleitung sowie die Bereichsleitungen.
- Für jeden pflegebedürftigen Bewohner wird eine Pflegedokumentation angelegt. Sie umfasst alle pflegerelevanten Daten wie z. B. Diagnose- und Anamnesedaten sowie die geplanten und durchgeführten Leistungen (Ziele, Verlauf, Ergebnisse) mit Angabe des Durchführenden und des Zeitpunkts der Leistungserbringung.
- Die Dokumentation über die Pflege muss vollständig sein, sie darf nicht einzelne Schritte auslassen. Die Aufzeichnung erfolgt durch die Pflegekräfte in zeitlich unmittelbarem Zusammenhang mit der Erbringung der Pflegeleistungen.
- Mit der Pflegedokumentation und sonstigen Bewohnerunterlagen ist sorgsam umzugehen, so dass eine Einsicht Unbefugter vermieden wird (z. B. durch gesicherte Aufbewahrung).

Auskünfte über Bewohner/Patienten und Einsicht in Bewohner-/ Patientenakten

- Auskünfte oder Übermittlungen von Bewohner-/Patientendaten (z. B. Besucher, Angehörige, Anrufer, Polizei, Staatsanwaltschaft etc.) sind nur zulässig, wenn es dazu eine gesetzliche Erlaubnis gibt oder wenn die Einwilligung des Bewohners bzw. seines gesetzlichen Vertreters vorliegt.
- Zu den schützenswerten Bewohnerdaten zählen nicht nur die Pflegedokumentation, sondern bereits die Identitätsdaten des Bewohners.
- Für die Rechtmäßigkeit von Auskünften und Übermittlungen ist die Einrichtungs- bzw. Pflegedienstleitung verantwortlich.
- Auskünfte oder Übermittlungen an Dritte erfolgen – sofern zulässig – grundsätzlich in schriftlicher Form. Beim Versand per Post ist auf die korrekte Adressierung zu achten.
- Auskünfte an Dritte werden grundsätzlich nicht am Telefon gegeben. Ausnahmen sind nur in dringenden Fällen zulässig, wenn der Dritte zweifelsfrei identifiziert werden kann (z. B. an bekannter Stimme und Telefonnummer im Display des Telefons).
- Die Erteilung von Auskünften durch Mitarbeiter an Ärzte, die mit der Behandlung des Bewohners befasst sind, ist erlaubt, wenn dies zur Behandlung erforderlich ist, der Bewohner die Einwilligung bei Heimeinzug gegeben hat und nach Hinweis auf die beabsichtigte Übermittlung nicht widersprochen hat.
- An einen Bevollmächtigten oder gerichtlich bestellten Betreuer dürfen Auskünfte über Angelegenheiten eines Bewohners erteilt sowie Akteneinsicht gewährt werden, sofern er sich ausweist und seine Vollmachtsurkunde bzw. seine gerichtliche Bestellung zum Betreuer vorlegt. Sofern die Auskunft Angaben über den Gesundheitszustand enthalten soll oder Einsicht in die Pflegedokumentation verlangt wird, muss in der Vollmacht bzw. in der

Bestellung zum Betreuer das Aufgabengebiet „Gesundheitssorge“ (bzw. Gesundheitsfürsorge) explizit genannt sein.

- Die Unterrichtung von Angehörigen ist zulässig, soweit es zur Wahrung ihrer berechtigten Interessen erforderlich ist, schutzwürdige Belange des Bewohners nicht beeinträchtigt werden und die Einholung der Einwilligung für den Bewohner gesundheitlich nachteilig wäre oder nicht möglich ist.
- Grundsätzlich haben gesetzliche Pflegekassen kein Auskunftsrecht bezogen auf die Pflegedokumentation eines Bewohners (mit Ausnahme des Teils „Leistungsnachweis“ der Pflegedokumentation). Diesbezügliche Anfragen der Pflegekassen werden mit dem Hinweis zurückgegeben, dass die Anfrage aus datenschutzrechtlichen Gründen (§§ 112 ff. SGB XI) über den Medizinischen Dienst der Krankenversicherung zu leisten ist.
- Der Medizinische Dienst der Krankenversicherung (MDK) oder ein bestellter Sachverständiger des Landesverbands der Pflegekassen kann sich mit Anfragen an unsere Einrichtung wenden oder zum Zweck von Prüfungen tätig werden. Die Auskunfts- und Prüfungsrechte des MDK bzw. des Sachverständigen beziehen sich auf den Zweck der Qualitäts- und Abrechnungsprüfung. Der Mitarbeiter des MDK bzw. der Sachverständige hat die Rechtsgrundlage seines Auskunfts- oder Prüfungsbegehrens zu nennen. Auskunft oder Akteneinsicht wird nur von der Einrichtungs- bzw. Pflegedienstleitung im erforderlichen Umfang gewährt.
- Die Heimaufsicht ist befugt, Prüfungen und Besichtigungen in der Einrichtung während der üblichen Geschäftszeiten vorzunehmen und dabei die Beschäftigten zu befragen. Die Heimaufsichtsbehörde darf bei Prüfungen vor Ort in alle zum Geschäftsbetrieb gehörenden Unterlagen Einsicht nehmen. Dazu zählen z. B. Personallisten, Dienstpläne, Unterlagen über die Qualifikation des eingesetzten Pflegepersonals, Heimverträge sowie auch die Pflegedokumentation. Selbst wenn hierbei im Einzelfall Daten zugänglich gemacht werden, die der ärztlichen Schweigepflicht unterliegen, ist dies durch das Heimgesetz ausdrücklich erlaubt.
- Mitarbeiter dürfen Anfragen (in der Regel Angehörige oder Besucher) nur Auskunft über den Aufenthaltsort eines Bewohners geben, sofern dieser dem nicht widersprochen hat.

Umgang mit Arbeitsplatzrechnern (PCs)

- Das Exportieren personenbezogener Daten auf externe Datenträger oder Geräte (z. B. Disketten, CDs, USB-Sticks, digitale Kameras) ist außer für Mitarbeiter, die mit Aufgaben der IT-Systemverwaltung besonders betraut sind, grundsätzlich untersagt. Das Einbringen von Daten oder Software über externe Datenträger oder Geräte in IT-Systeme ist ebenso untersagt.
- Aus Sicherheitsgründen sind Diskettenlaufwerke und andere Geräte oder Schnittstellen von PCs (z. B. USB-Schnittstellen), die einen Datenexport oder –import erlauben, soweit technisch möglich deaktiviert oder ausgebaut.
- Bei wichtigen dienstlichen Erfordernissen des Imports oder Exports von Daten wenden Sie sich an die Heimverwaltung.
- Bei vernetzten PCs sind die Daten grundsätzlich auf einem zentralen Laufwerk zu speichern. Datenbestände auf der lokalen Festplatte (Laufwerk C:) werden nicht automatisch gesichert.
- Änderungen an den IT-Geräten, der installierten Software oder der Verkabelung sind nur in Abstimmung mit der Heimverwaltung zulässig.

Umgang mit Passwörtern

- Passwörter sind nirgends zu notieren und niemandem mitzuteilen.
- Ein Passwort darf nur dem Benutzer bekannt sein.
- Passwörter sollen eine Mindestlänge von ***10-20*** Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben mit Groß-/Kleinschreibung, Zahlen und mindestens einem Sonderzeichen) zu gestalten.

- Passwörter dürfen nicht leicht zu erraten sein. Vor- und Familiennamen oder Geburtstage sind nicht zur Bildung von Passwörtern geeignet. Trivialpasswörter (wie
- z. B. 4711, 12345 oder andere nebeneinander liegende Tasten) dürfen nicht verwendet werden.
- Einmal genutzte Passwörter sind nicht wieder zu verwenden.
- Die Weitergabe der eigenen Benutzererkennung und des eigenen Passworts an Dritte (auch Vorgesetzte) ist unzulässig.
- Wenn der Verdacht besteht, dass die eigenen Zugangs- und Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist das Passwort umgehend zu ändern und ein Mitarbeiter der Verwaltung zu benachrichtigen.
- Passwörter dürfen nicht als Teil eines automatischen Anmeldeprozesses verwendet werden, sofern dies nicht durch technische Vorgaben seitens des Softwareherstellers erzwungen wird.

Richtlinie zu mobilen IT-Geräten, Smartphones und Mobiltelefonen

- Grundsätzlich sollen Bewohnerdaten und Mitarbeiterdaten nicht auf mobilen IT-Geräten wie Notebooks verarbeitet werden.
- Aus wichtigem Grund können personenbezogene Daten auf mobilen IT-Geräten verarbeitet werden, wenn zuvor der Inhalt der gesamten Festplatte durch einen dafür zuständigen Mitarbeiter verschlüsselt wurde.
- Mobile IT-Geräte müssen gegen Diebstahl und unbefugten Zugriff gesichert aufbewahrt werden.
- Das Mitführen von Mobiltelefonen und Smartphones ist während der Dienstzeit grundsätzlich verboten. Die Nutzung ist nur in den Pausen gestattet! In besonders dringenden Fällen ist der nächste Vorgesetze zu informieren, wenn der Einsatz des Handy´s notwendig ist.
  (Siehe auch Mitarbeiterregeln)

Aufbewahrung, Transport und Vernichtung von Datenträgern

- Datenträger, die personenbezogene Daten enthalten, sind gesichert aufzubewahren. Hierfür verantwortlich ist der externe Dienstleister, der einen Dienstleistungsvertrag besitzt..

Regelung zu Versand und Empfang von Telefaxen

Bei der Übertragung von Informationen per Telefax ist die Vertraulichkeit der Daten gefährdet, weil

- o die Informationen „offen“, das heißt unverschlüsselt, übertragen werden und
- o sensible personenbezogene Daten durch Adressierungsfehler in falsche Hände geraten können.

Die Verantwortung für die vertrauliche Übermittlung (Schweigepflicht und Datengeheimnis) liegt beim Absender des Telefaxes. Daher sind bei der Übermittlung von Dokumenten per Telefax die folgenden Regeln einzuhalten:

- Es gilt der Grundsatz: Was am Telefon aus Gründen der Geheimhaltung nicht gesagt werden darf, darf auch nicht gefaxt werden.
- Telefax-Geräte oder PCs, mit denen Faxe verschickt oder empfangen werden, sind so aufzustellen, dass die Vertraulichkeit eingehender Faxe gewährleistet ist.
- Sensible personenbezogene Daten – insbesondere Gesundheitsdaten der Bewohner – dürfen nur dann per Telefax übertragen werden, wenn dies von der Eilbedürftigkeit her geboten ist und Sie zuvor mit dem Empfänger den Sendezeitpunkt abgestimmt haben, so dass das Fax nicht in falsche Hände geraten kann (z.b. Ärzte oder Krankenhaus).
- Sicherheitsmaßnahmen, die das Telefaxgerät selbst bietet, sollten genutzt werden, zum Beispiel Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung oder Abruf nur nach Passwort.
- Telefaxe sind deutlich zu adressieren, mit Empfängername, Telefax- und Telefon-Nummer. Der Absender ist mit Fax- und Telefon-Nummer sowie Anzahl der gesendeten Seiten anzugeben.

- Die vom Empfängergerät vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu prüfen, damit bei Wählfehlern die Übertragung unverzüglich abgebrochen werden kann.
- Telefaxe mit sensiblen Daten sollten nicht außerhalb der üblichen Dienstzeiten des Empfängers gesendet werden. Das Fax kann beim Empfänger offen liegen bleiben und in falsche Hände geraten.

Fotos/ Einwilligung

Die Rechtsgrundlage für die Veröffentlichung von Fotos im Internet bildet das Kunsturhebergesetz (KunstUrhG), welches das Recht am eigenen Bild beschreibt. Hiernach dürfen gem. § 22 Satz 1 Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die rechtlichen Bestimmungen des KunstUrhG gelten für Jedermann, also für Bewohner/Patienten, Angehörige, Mitarbeiter und auch für ggf. unbeteiligte Dritte. D. h., wenn Bilder eingestellt werden sollen, gilt die Einwilligungserfordernis für sämtliche abgebildeten Personen.
Ausnahmen zu § 22 KunstUrhG, bei denen Fotos ohne Einwilligung veröffentlicht werden dürfen, gelten bei
- Bildnissen aus dem Bereich der Zeitgeschichte;
- Bildern, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen oder
- Bildern von Versammlungen, Feierlichkeiten und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben.

Für unsere Einrichtung liegen diese Ausnahmen nicht vor. Somit ist die Vorlage einer Einwilligung zwingende Voraussetzung für die Einstellung von Fotos im Internet oder in Zeitschriften. Die Einwilligung bedarf grundsätzlich der Schriftform. Sie ist möglichst präzise zu fassen. In ihr ist anzugeben, zu welchem Zweck diese Einwilligung erteilt wird (Fotos von Veranstaltungen wie Sommerfest, Geburtstagsfeier etc.). Weiterhin sind die Medien, in denen die Veröffentlichung geplant ist, genau aufzuführen (Internet, Zeitung, Aushänge in der Einrichtung, etc.).

Aufbewahrungsfristen von Daten und Dokumenten

	Aufbewahrungsfrist	**Gesetze**
Bewohnerakten	30 Jahre	§ 199 II BGB
Steuerunterlagen	10 Jahre	§ 357 HGB
Rechnungen/ kaufmännische Unterlagen	10 Jahre	§ 147 AO
Geschäftsbriefe	6 Jahre	§ 147 AO
Preisverzeichnisse	6 Jahre	§ 147 AO
Dokumentationsmaterial	5 Jahre	DSG
Pflegehandbücher, Qualitätshandbücher	5 Jahre	DSG
Standards, Leitlinien, Empfehlungen	5 Jahre	DSG
Mitarbeiterunterlagen (Personalakte)	3 Jahre	§ 195 BGB

Aus dem BGB § 199: Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen, verjähren ohne Rücksicht auf ihre Entstehung, Kenntnis oder grob fahrlässige Unkenntnis in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, den Schaden auslösenden Ereignis an.

Impressumspflicht Internet
Die Impressumspflicht (§ 5 TMG) für unsere Website berücksichtigt alle gesetzlichen Vorgaben wie:
- Name und Anschrift der Einrichtung
- bei juristischen Personen der oder die jeweils Vertretungsberechtigter
- Kontaktdaten
- Register/Registernummer
- Umsatzsteueridentifikationsnummer
- Zusätzliche Regelungen für bestimmte Berufe

Internet/ E-Mail Nutzung durch Mitarbeiter
- Die Nutzung von Mail und Internet am Arbeitsplatz erfolgt ausschließlich zu dienstlichen Zwecken.
- Das Senden und empfangen privater Mails ist nicht erlaubt.

Umgang mit der Post
Die Wahrung des Post- und Briefgeheimnisses ist ein wichtiges Anliegen in unserer Einrichtung. Es gelten nachfolgende Regelungen:
Folgende Eingangspost darf NICHT geöffnet werden und ist unmittelbar an den Empfänger weiterzuleiten:
- Vermerke mit der Kennzeichnung „vertraulich“ oder „persönlich“
- Adressierungen zuerst mit Name, Vorname und erst anschließend Unternehmensbezeichnung
- Post an die „Geschäftsleitung“ oder namentlich Herrn/Frau (Namensliste)
- Eingangspost, die für die Personalabteilung bestimmt ist, oder namentlich …
- Korrespondenz an die Mitarbeitervertretung oder namentlich ….
- Briefe, die an den betrieblichen Datenschutzbeauftragten adressiert sind, oder namentlich …
- Eingangspost von Banken ist ungeöffnet an die Finanzabteilung zu übergeben
- Bewohnerpost, diese ist unverzüglich dem Bewohner oder seinem Vertretungsberechtigten zuzustellen

Folgende Post darf GEÖFFNET werden und ist an den Empfänger weiterzuleiten:
- Adressierung zuerst mit dem Namen der Einrichtung
- Werbepost

Mitgeltende Dokumente:
Heimvertrag inkl, Einwilligungsklausel
F 4.7 GES FB 144 Einwilligung Bew. für Foto-Film
F 4.7 GES FB 145 Einwilligung MA für Foto-Film
F 4.7 GES FB 146 Einwilligung Bewerbungsverfahren

Mit diesem Thema im Zusammenhang stehen:
F 2.5 Stellen- und Aufgabenbeschreibung, F 2.6 Einarbeitung neuer Mitarbeiter, F 2.8 Fort- und Weiterbildung
F 3.2 Lenkung von Dokumenten und Aufzeichnungen, F 4.1 Umgang mit Kundeneigentum,
K 1.5 Pflegedokumentationssystem,
U 1.6 Verwaltung der Kundendaten, U1.7 Verwaltung der Personaldaten, U2 Öffentlichkeitsarbeit

Bearbeitet von:	Geprüft von:	Datum:	Freigabe durch:
C. Hallmann M. Rupil	C. Hallmann	25.06.2018	B. Schwalfenberg