Letzte Änderung: 05.08.2021
Autor: Nico-Eugen Lange

SENIORENWOHNZENTRUM
VIADUKT

Datenschutzkonzept

Der Seniorenwohnzentrum Viadukt GmbH

Einleitung

Die Seniorenwohnzentrum Viadukt GmbH ist eine vollstationäre Pflegeeinrichtung im Erholungsort Zierenberg, einer Kleinstadt mitten im Naturpark Habichtswald zwischen dem Hohen Dörnberg und dem großen Bärenberg.

In unserem kleinen Seniorenwohnzentrum leben 33 Menschen der verschiedenen Pflegegrade in Familiärer Atmosphäre, um diese Atmosphäre zu wahren ist auch der Schutz Personenbezogener Daten von äußerster Notwendigkeit damit sich unsere Bewohner und Mitarbeiter bei uns wohlfühlen, diesem wollen wir gerecht werden.

Unser Datenschutzkonzept beruht auf den in Art 5 Z 1 DSGVO formulierten Grundsätzen wie Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität, Recht auf Vergessenwerden und Vertraulichkeit und ist rechtmäßig (Art 6 DSGVO). Die von der DSGVO geforderte Einhaltung der Verordnungskonformität (Art. 5 Z 2; Art 24 Z 1), der Einhaltung der Betroffenenrechte (Art 13-20), der Meldepflicht bei Datenschutzverletzung (Art 33-34), der Nachweis- und Rechenschaftspflicht (Art 5 Z 2, Art 24 Z 1) ist gewährleistet. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt (Art 32 Z 1), u.a. basierend auf der Checkliste, enthalten im letzten Kapitel dieses Datenschutzkonzeptes

Verhältnis zu gesetzlichen Anforderungen

Dieses Datenschutz und Sicherheitskonzept ersetzt nicht EU-Vorschriften und die nationalen Gesetze. Sie ergänzt die nationalen Datenschutzgesetze. Diese Vorschriften und Gesetze haben Vorrang, wenn die Einhaltung dieser Richtlinie zu einem Verstoß gegen nationales Recht führen würde. Der Inhalt dieser Richtlinie ist auch dann zu beachten, wenn es keine entsprechenden nationalen Gesetze gibt. Sofern die Einhaltung dieser Richtlinie zu einem Verstoß gegen nationales Recht führen würde oder nach nationalem Recht abweichende Regelungen zu dieser Richtlinie erforderlich sind, ist dies dem Geschäftsführer und dem Datenschutzbeauftragten der Seniorenwohnzentrum Viadukt GmbH für den Datenschutz zu melden. Im Falle von Konflikten zwischen nationaler Gesetzgebung und dieser Richtlinie werden der Datenschutzbeauftragte und die Geschäftsführung mit der zuständigen Aufsichtsbehörde zusammenarbeiten, um eine praktische Lösung zu finden, die dem Zweck dieser Richtlinie entspricht.

Letzte Änderung: 05.08.2021
Autor: Nico-Eugen Lange

Verantwortlichkeiten im Unternehmen

Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Daten-Verarbeitung bei der Seniorenwohnzentrum Viadukt GmbH trägt der Geschäftsführer als Vertreter der verantwortlichen Stelle

Verantwortlich für das vorliegende Datenschutzkonzept sind:

Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO
Seniorenwohnzentrum Viadukt GmbH
Heiko Fuchtmann
Kasseler Straße 46
34289 Zierenberg
Tel: 05606 1067
E-Mail: Fuchtmann@swz-viadukt.de

Datenschutzbeauftragter gemäß Art. 37 ff. DSGVO
Seniorenwohnzentrum Viadukt GmbH
Nico-Eugen Lange
Kasseler Straße 46
34289 Zierenberg
Tel: 05606 1067
E-Mail: dsb@swz-viadukt.de

Vertretung des Datenschutzbeauftragten
Seniorenwohnzentrum Viadukt GmbH
Katharina Jordan
Kasseler Straße 46
34289 Zierenberg
Tel: 05606 1067
E-Mail: hl@swz-viadukt.de

Die verantwortliche Stelle ist dabei insbesondere für den Erlass von Dienstanweisungen und Regelungen zum Datenschutz und zur Datensicherheit zuständig. Dies gilt sowohl für den allgemeinen, konventionellen Datenschutz als auch für den technischen Datenschutz.

Für die Einhaltung der jeweils anzuwendenden Vorschriften zum Datenschutz und zur Datensicherheit ist der Geschäftsführer zusammen mit dem Datenschutzbeauftragten und der Heimleitung der Einrichtung zuständig und verantwortlich.

Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Missverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu vermeiden und gegebenenfalls aufzulösen. Alle Regelungen sollten deshalb auch ein Erstellungsdatum oder eine Versionsnummer enthalten.

Überwachung

Die Überwachung und Prüfung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen obliegt der verantwortlichen Stelle. Die Personalvertretung sowie die/der Datenschutzbeauftragte ist entsprechend zu beteiligen. Die Ergebnisse sind im Rahmen der Dokumentationspflicht schriftlich festzuhalten.

Fortschreibung

Das Datenschutzkonzept ist im Zusammenhang mit den technisch organisatorischen Maßnahmen (Art. 24 ff. EU-DSGVO) regelmäßig fortzuschreiben. Dabei ist zu prüfen, ob sich die Datensicherheitsmaßnahmen bewährt haben.

Inkrafttreten

Das Datenschutzkonzept wurde am 05.08.2021 finalisiert und für die Zustimmung des Inkrafttretens an die Heimleitung und die Geschäftsführung übergeben.

Weiterbildung und Stand der Technik

Die Mitarbeiterinnen und Mitarbeiter sind über die datenschutzrechtlichen Vorschriften zu unterrichten und zu schulen.

Die Kenntnisse über die in der Tätigkeit des Mitarbeiters liegenden Datenschutz-bestimmungen hat sich der Mitarbeiter durch entsprechende Fortbildungen anzueignen (jeweils anzuwendende Fachgesetze).

Die Unterrichtung ist aktenkundig zu machen und zur Personalakte zu nehmen.

Datenschutzrechtliche Vorschriften müssen fester Bestandteil der Fortbildungsplanung der jeweiligen Organisationseinheiten sein. Dies schließt auch die Fortbildung im Umgang mit technikunterstützter Informationsverarbeitung und den daraus resultierenden Datensicherheitsmaßnahmen ein.

Aktivitäten	*Veranstalter*	*Sonstiges*
Info.-Weiterbildungsveranstaltungen	*Webinare, etwa bei Datenschutz-guru.de und ebenfalls regelmäßige Schulungen in unserer Einrichtung*	*regelmäßig*
Info Homepages und Newsletter zur DSGVO für unsere Mitarbeiter	*https://www.datenschutz.de*	*Homepage*
	www.datenschutz-guru.de	*Newsletter*

Sensibilisierung der Mitarbeitenden / Dienstleister

Besonders wichtig ist die Sensibilisierung aller relevanten Mitarbeitenden. Nur mit informierten und achtsamen Mitarbeitenden können Sicherheitsmaßnahmen zur DSGVO wirksam umgesetzt und eventuelle Sicherheitsvorfälle rechtzeitig erkannt werden. Sobald die Ursache eines Sicherheitsvorfalls identifiziert wurde, müssen Maßnahmen zu dessen Behebung ergriffen werden. Die Behebung von Sicherheitsvorfällen muss ausführlich dokumentiert werden. Ein Beispiel für eine Sensibilisierung / Verpflichtung auf Einhaltung der DSGVO der Mitarbeitenden befindet sich im Anhang. Ebenfalls im Anhang: Ein Mustervertrag zur Auftragsdatenverarbeitung.

Tür- und Fenstersicherung

Die Seniorenwohnzentrum Viadukt GmbH ist eine offene Altenpflegeeinrichtung und verfügt über keine geschlossene Abteilung, aufgrund dessen ist die Eingangstür für unsere Bewohner, Angestellten und Besucher immer geöffnet und hat keine Zutrittsbeschränkung.
Fenster zu Räumen mit DSGVO relevanten Daten sind mit einem Sichtschutz ausgestattetet.

Aktenführung und Aktenaufbewahrung

Akten, in denen personenbezogene Daten verarbeitet werden, sind so aufzubewahren, dass eine Einsichtnahme durch unbefugte Dritte nicht möglich ist. Sie sind grundsätzlich in

Schränken oder anderen zur Aktenaufbewahrungen geeigneten Möbeln aufzubewahren. Dies gilt auch für Vorgänge, die in der laufenden Bearbeitung sind (Clear-Desk- Anweisung)

Bei Akten, die einem besonders schutzwürdigen Interesse unterliegen, entscheidet die jeweilige Organisationseinheit über die darüber hinaus erforderliche Form der Aufbewahrung.

Papierabfälle, die personenbezogenen Daten enthalten, sind in den lokalen Aktenvernichtern, oder den dafür vorgesehenen Behältnissen zu entsorgen.

Archiv und Aufbewahrungsfristen

Die Aufbewahrung von Akten im Archiv ist bereichsbezogen durchzuführen.

Akten, die einem besonders schutzwürdigen Interesse unterliegen (z.B. Personal- und Bewohnerakten) sind vor der Einsichtnahme durch unbefugte Dritte besonders zu sichern.

Akten und die damit verarbeiteten personenbezogenen Daten sind grundsätzlich zu löschen, wenn sie für die Aufgabenerledigung nicht mehr erforderlich sind und Aufbewahrungsfristen nicht entgegenstehen. Dies betrifft sowohl elektronisch, als auch in Papier geführte Akten.

Die Akten sind einer Vernichtung (z.B. Schreddern) zuzuführen, bei der gewährleistet ist, dass unbefugte Dritte keine Einsicht nehmen können.

Soweit keine gesetzlichen Aufbewahrungsfristen bestehen, sind grundsätzlich die aktuellen Aufbewahrungsempfehlungen der KGSt, in der jeweils vorliegenden Fassung anzuwenden.

den Ablauf der Frist überwacht die für die Aktenführung zuständige Fachabteilung.

Datenverarbeitungen/Datenverarbeitungszwecke

Zwecke und Beschreibung der Datenverarbeitungen:

Pflegedokumentation:
Für die entsprechende Pflege und Betreuung der Bewohner dürfen personenbezogene Daten verarbeitet werden, es werden auch Daten der besonders zu schützenden Kategorie wie Gesundheitsdaten der Bewohner verarbeitet um die Medizinische Versorgung sicher zu stellen.

Mitarbeiterdaten, Datenverarbeitung für das Arbeitsverhältnis
Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses erforderlich sind. Für die Entscheidung über die Begründung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsverhältnisses bezogen sein.

Die Verarbeitung von Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

Rechnungswesen und Geschäftsabwicklung:
Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit unserem Steuerbüro, Bewohnern, Betreuern, Krankenhäusern, Krankenkassen sowie

Lieferanten. sowie an der Geschäftsabwicklung mitwirkende Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten.

Kundenbetreuung und Marketing:
Serviceorientierte Information und Betreuung von kategorisierten Kunden, Lieferanten und an der Geschäftsabwicklung mitwirkende Dritte bzw. Geschäftspartner inkl. deren jeweiligen Kontaktpersonen und Interessenten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie Übermittlung von Newsletter, Serienbriefe und Infomaterial.

Reinigungspersonal

Das Reinigungspersonal darf nur den Büro- und Arbeitsraum öffnen, in dem die Reinigung erfolgen soll.

Die Kontrolle der Einhaltung dieser Vorschriften ist sicherzustellen.

Verstöße sind der Fachabteilung für die Vergabe der Reinigungsstellen unverzüglich zu melden

Publikumsverkehr

Es ist sicherzustellen, dass Besucher der Einrichtung bei ihrer Vorsprache in der jeweiligen Fachabteilung andere, als die ihre Angelegenheit betreffende personenbezogene Daten, nicht zur Kenntnis nehmen können. Dies gilt sowohl für Daten in Akten, als auch für automatisiert verarbeitete Daten.

Computermonitore sind so aufzustellen, dass sie für Dritte nicht einsehbar sind.

Auskünfte, Datenübermittlung

Bei einer Auskunftserteilung bzw. Datenübermittlung ist die Identität der bzw. des Ersuchenden zu prüfen, sollte also ein Auskunftsberechtigter in unserer Einrichtung anrufen oder vorstellig werden, ist es vor der Auskunftserteilung zwingend notwendig die Identität zu bestätigen.

Die jeweiligen Fachabteilungen entscheiden selbständig über die Erforderlichkeit und die Festlegung von einheitlichen Verfahrensregelungen für die Auskunftserteilung bzw. Übermittlung von personenbezogenen Daten an Dritte

Datenschutz-Folgenabschätzung

Die Seniorenwohnzentrum Viadukt GmbH analysiert bei der Einführung neuer Verarbeitungsvorgänge oder bei einer wesentlichen Änderung eines bestehenden Verarbeitungsvorganges vor der Verarbeitung, ob diese Verarbeitung ein hohes Risiko für die Privatsphäre der Betroffenen darstellt. Dabei sind Art, Umfang, Kontext und Zweck der Datenverarbeitung zu berücksichtigen. Im Rahmen der Risiko Evaluierung führt der verantwortliche Datenschutzbeauftragte in unserer Einrichtung eine Bewertung der Auswirkungen der geplanten Verarbeitungen auf den Schutz personenbezogener Daten 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 Geschäftsführer darüber informiert werden, damit er die zuständige Datenschutzaufsichtsbehörde konsultieren kann.

Impressum und Datenschutzerklärungen

DSGVO-konform auf unserer Unternehmens Webseite : www.swz-viadukt.de/impressum/

Letzte Änderung: 05.08.2021
Autor: Nico-Eugen Lange

Betroffenenrechte wahren

Grundsätzlich stellen wir jedem Nutzer bzw. Betroffenen die jeweils aktuelle Version unseres Datenschutzkonzeptes auf unserer Homepage im Sinne von Transparenz und Vertrauen zum Download bereit (www-swz-viadukt.de/Datenschutzkonzept/). Gemäß der DSGVO hat jeder Betroffene folgende Rechte: • Recht auf Auskunft (Art 15 DSGVO) • Recht auf Berichtigung (Art 16 DSGVO) • Recht auf Löschung (Art 17 DSGVO) • Recht auf Einschränkung (Art 18 DSGVO) • Recht auf Übertragbarkeit (Art 20 DSGVO) • Recht auf Widerspruch (Art 21 DSGVO) • Recht auf Beschwerde bei der Datenschutzbehörde

Betroffenenrechte

Alle in diesem Punkt aufgeführten Rechte der Betroffenen und Pflichten der Seniorenwohnzentrum Viadukt GmbH sind für den Betroffenen drittbegünstigend. Die nach diesem Punkt gerichteten Anfragen und Beschwerden müssen innerhalb von einem Monat beantwortet werden. Unter Berücksichtigung der Komplexität und der Anzahl der Anträge kann dieser Zeitraum von einem Monat um höchstens zwei weitere Monate verlängert werden, worüber der Betroffene entsprechend unterrichtet werden muss

Ein Betroffener hat gegenüber der Seniorenzentrum Viadukt GmbH folgende Rechte, wie sie in den näheren Einzelheiten des EU-Rechts festgelegt sind:
» das Recht, über die Umstände der Verarbeitung seiner personenbezogenen Daten informiert zu werden. Die Vorgaben des Datenschutzbeauftragten an derartige Informationen sind zu beachten.
» das Recht auf Auskunft darüber, in welcher Art und Weise seine Daten verarbeitet werden und welche Rechte ihm insofern zustehen. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht spezifische Einsichtsrechte in Unterlagen des Arbeitgebers (z. B. Personalakte) vorgesehen sind, so bleiben diese unberührt. Auf Wunsch erhält der Betroffene (ggf. gegen ein angemessenes Entgelt) eine Kopie seiner personenbezogenen Daten, es sei denn, schutzwürdige Interessen Dritter stehen dem entgegen.
» das Recht auf Berichtigung oder Ergänzung personenbezogener Daten, sollten diese unrichtig oder unvollständig sein.
» das Recht auf Löschung seiner Daten, wenn er seine Einwilligung widerruft oder die Rechtsgrundlage für die Verarbeitung der Daten fehlt bzw. weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.
» das Recht auf Einschränkung der Verarbeitung seiner Daten, wenn er die Richtigkeit bestreitet oder die Daten von der Seniorenzentrum Viadukt GmbH nicht mehr benötigt werden, aber der Betroffene die Daten für seine Rechtsansprüche braucht. Der Betroffene kann zudem verlangen, dass die Seniorenwohnzentrum Viadukt GmbH die Verarbeitung seiner Daten einschränkt, wenn sie ansonsten die Daten löschen müsste oder wenn sie einen Widerspruch des Betroffenen prüft.
» das Recht, die ihn betreffenden und von ihm auf Grundlage einer Einwilligung oder im Rahmen eines mit ihm geschlossenen oder angebahnten Vertrages bereitgestellten personenbezogenen Daten in einem gängigen digitalen Format zu erhalten und dieses an einen Dritten zu übermitteln, soweit die Verarbeitung mithilfe automatisierter Verfahren erfolgt und dies technisch machbar ist.
» das Recht, der Verarbeitung auf der Rechtsgrundlage überwiegender Interessen der Seniorenzentrum Viadukt GmbH oder Dritter zu widersprechen, wenn hierfür Gründe aus seiner besonderen persönlichen Situation vorliegen. Das Widerspruchsrecht besteht allerdings nicht, wenn die Seniorenwohnzentrum Viadukt GmbH zwingende Gründe für die Verarbeitung hat oder wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Im Fall eines berechtigten Widerspruchs sind die Daten zu löschen.

Beschwerdeverfahren

Betroffene sind berechtigt, eine Beschwerde bei dem Datenschutzbeauftragten einzureichen, wenn sie der Ansicht sind, dass gegen diese Richtlinie verstoßen wurde. Solche Beschwerden können per E-Mail an dsb@swz-viadukt.de, schriftlich per Post, oder Schriftlich persönlich eingereicht werden. Für den Fall, dass der Betroffene mit der Entscheidung der Seniorenzentrum Viadukt GmbH über die Einhaltung der Vorschriften nicht einverstanden ist (oder aus anderen Gründen mit ihrer Handhabung nicht zufrieden ist), steht es ihm frei, diese Entscheidung oder dieses Verhalten durch Ausübung seiner Rechte anzufechten. Dazu kann er sich an die zuständige Aufsichtsbehörde wenden, insbesondere in dem Land seines gewöhnlichen Aufenthaltsortes, seines Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, oder Klage bei Gericht erheben. Weitergehende gesetzliche Rechte und Zuständigkeiten bleiben hiervon unberührt.

Meldung von Datenschutzverletzungen: Prozesskette

1. *Meldung einer Datenschutzverletzung an die zuständige Stelle*
2. *Prüfung des Sachverhaltes durch die zuständige Stelle*
3. *Erste Dokumentation der Verletzung an den Datenschutzbeauftragten der Einrichtung*
4. *Risiko-Evaluierung der Datenschutzverletzung durch den Datenschutzbeauftragten*
5. *Erstellung einer Datenschutzverstoß Dokumentation und umzusetzende Maßnahmen*
6. *Wenn nötig Meldungserstattung der Datenschutzverletzung durch den Datenschutzbeauftragten an die Aufsichtsbehörde Hessen*
7. *Weitergabe der vom Datenschutzbeauftragten erstellten Dokumentation an die Heimleitung oder Geschäftsführung für die Umsetzung notwendiger Maßnahmen (Weisungsbefugnis)*
8. *Erstellen einer abschließenden Dokumentation und Meldung an alle Beteiligten nach Abschluss der Maßnahmen*

(Für die Bearbeitung gemeldeter Datenschutzverletzungen wird je nach Klassifizierung der Verletzung eine Bearbeitungszeit von bis zu 4 Wochen berechnet)

Verfahren

Die eingesetzten Verfahren sind in eine Bestandsliste aufzunehmen (Verzeichnis von Verarbeitungstätigkeiten, Art. 30 EU-DSGVO).
Folgende Angaben müssen enthalten sein:

1. *den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragte*
2. *die Zwecke der Verarbeitung;*
3. *eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;*
4. *die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;*
5. *gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Abs. 1 Unterabschnitt 2 DSGVO genannten Datenübermittlung die Dokumentierung geeigneter Garantien*
6. *wenn möglich die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;*
7. *wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1*

- *Die Rechte für den Zugriff auf die Verfahren sind von der Geschäftsführung und dem Datenschutzbeauftragten der Seniorenwohnzentrum Viadukt GmbH zu regeln. Sie sind innerhalb der Verfahren auf das notwendige Maß zu beschränken.*

Letzte Änderung: 05.08.2021
Autor: Nico-Eugen Lange

SENIORENWOHNZENTRUM
VIADUKT

Sicherheitskonzept für die automatisierte Datenverarbeitung

Der Seniorenwohnzentrum Viadukt GmbH

EDV

Der EDV-Beauftragte der Seniorenwohnzentrum Viadukt GmbH stellt den Einsatz und den Betrieb der IT Systeme sicher.

Ein Zugriff auf verschlüsselte Datenbestände darf nur unter Beteiligung autorisierter Mitarbeiterinnen und Mitarbeiter der Einrichtung erfolgen. Gleiches gilt für den im Bedarfsfall notwendigen Zugriff auf Userprofile.

Ein Zugriff auf das Persönliche Email Postfach, ohne Anwesenheit des Besitzers, ist nur in Ausnahmefällen unter Aufsicht – nach dem sechs Augen Prinzip - mit dem Datenschutzbeauftragten und dem Geschäftsführer abzustimmen und zu dokumentieren.

PC-Benutzer/-innen

Die PC-Benutzerinnen und PC-Benutzer sind vor Aufnahme der Arbeit an PCs umfassend zu schulen.

Ihnen sind entsprechende Anleitungen zur Verfügung zu stellen um die Firmensoftware zu verwenden.

Die PC-Benutzerinnen und PC-Benutzer sind selbst für die ordnungsgemäße Nutzung, der ihnen zur Verfügung gestellten Hard- und Software zuständig.

Sie sind über die grundsätzliche Speicherinfrastruktur aufzuklären.

Kennwörter

Für alle PC-Benutzerinnen und PC-Benutzer sind Zugangskennungen für das Netzwerk und für die Verfahren zu vergeben.

Dabei sind neben Benutzernamen auch mindestens 8-stellige Kennwörter zu verwenden (genaue Passwortanforderungen werden systemseitig vorgegeben).

Kennwörter sind alle 90 Tage zu wechseln. Tipps für Passwörter sind im Anhang 2 beigefügt.

Die Anzahl der Anmeldeversuche ist auf maximal 10 zu begrenzen

Beim Verlassen des Arbeitsplatzes ist die passwortgeschützte Bildschirmsperre zu aktivieren. Dazu kann z.B. auf Windows Betriebssystemen die Tastaturkombination Windowstaste + L gedrückt werden. Die Bildschirmsperre wird nach 10 Minuten der Nichtnutzung des PC's automatisch aktiviert.

Hardware und Software

Die Hard.-Software ist generell von dem EDV-Beauftragten unseres Unternehmens zu beschaffen und zu installieren.

Bei Lieferung sind sämtliche Geräte durch Inventarisierung zu erfassen.

Aus dem Geräteverzeichnis müssen sich der Aufstellungsort, die Geräteart, der Gerätetyp, die Seriennummer und das Lieferdatum ergeben. Weitere Angaben können jederzeit ergänzt werden.

Ein Umstellen der Geräte innerhalb unserer Einrichtung ist im Geräteverzeichnis zu berichtigen.

Die Konfigurationsdaten der eingesetzten Hard- und Software (IP-Adressen etc.) sind vor unbefugtem Zugriff zu schützen.

Bei Entfernung der Geräte (Reparatur, Verschrottung etc.) ist der Verbleib zu notieren.

Vor einer Weitergabe an Dritte (z. B. Schulen, Verkauf an Mitarbeiter/innen) ist von der EDV-Abteilung sicherzustellen, dass die auf den Datenträgern gespeicherten Daten unwiederbringlich gelöscht sind. Sollte dies nicht möglich sein, sind die Datenträger auszubauen.

Es ist grundsätzlich Standardsoftware einzusetzen.

Die Originalsoftware ist durch die EDV-Abteilung gesichert aufzubewahren.

Private Hard- und Software darf in unserer Einrichtung unter Aufsicht des Datenschutzbeauftragten genutzt werden.

Die Regeln zur Nutzung von Privater Hard- und Software ist durch den Datenschutzbeauftragten festzulegen und mit der Geschäftsführung abzustimmen.

private Nutzung von dienstlicher Hard- und Software außerhalb der vorhandenen Dienstanweisungen für den Bereich EDV ist nicht zulässig

Letzte Änderung: 05.08.2021
Autor: Nico-Eugen Lange

Zentrale Rechner (Server)

Der Server ist soweit möglich in zentralen Serverräumen oder in einem abschließbaren, für den Serverbetrieb zugelassenen Schrank aufzustellen.

der Server ist mit einer unterbrechungsfreien Stromversorgung (USV) auszustatten, die Funktion des Servers ist in regelmäßigen Abständen zu überprüfen und zu protokollieren.

Die Festplatten der Server sind mind. als Raid-5-Systeme zu konfigurieren.

Der Server muss mit einer unterbrechungsfrei arbeitenden Antivirus-Software und einer Firewall auszustatten um Zugriffe auf Personenbezogene Daten von außen zu vermeiden und effektiv abzuwehren.

Es hat in regelmäßigen abständen ein Backup der wichtigsten Daten auf dem Server stattzufinden, dieses Backup kann auf einer externen verschlüsselten Festplatte abgelegt werden.

Netzstruktur/Verteiler

Die in der Seniorenwohnzentrum Viadukt GmbH vorhandene Netzstruktur ist in einer Übersicht zu dokumentieren (Nachweise über sämtliche IP-Ports, Benutzer, Telefon, PC, Drucker, Fax etc.).

Die Verteiler (wie Router, Hub und Switch) sind in verschlossenen, für den Netzwerkbetrieb zugelassenen Schränken zu betreiben.

Zentrale Drucker u. Kopierer

Werden Drucker für zentrale Druckaufträge genutzt, ist darauf zu achten, dass Ausdrucke mit personenbezogenen Daten nicht unbeaufsichtigt erfolgen, bzw. nach dem Ausdruck umgehend aus dem Gerät genommen werden.

Datenverwaltung

Alle Datenbestände sind nur über die jeweilige Speicherinfrastruktur entsprechend der geltenden Dienstanweisung zu sichern.

Die Daten sind durch Zugriffsrechte auf dem jeweiligen Server voneinander abzugrenzen.

Die dauerhafte Speicherung von Dateien als Muster oder Textbausteine ist nur zulässig, wenn sie anonymisiert werden bzw. keine Personenbezogenen Daten enthalten.

Dienstliche Daten dürfen nicht auf privaten Rechnern und private Daten nicht auf dienstlichen Rechnern gespeichert werden.

Datensicherung

Um die Verfügbarkeit und die Wiederherstellbarkeit der Daten auf den Servern zu gewährleisten, sind regelmäßige, inkrementelle Backups durchzuführen.

im Rahmen einer Monatssicherung hat ein zusätzliches umfangreicheres Backup stattzufinden.

Die Bänder sind diebstahl- und datensicher in besonderen Stahlschränken aufzubewahren.

Die Backup Funktion und die Wiederherstellung der Daten ist in regelmäßigen Abständen zu überprüfen und zu protokollieren.

Datenträger

Vorhandene USB-Schnittstellen und CD-Laufwerke sind soweit möglich, mittels eines Passwort geschützten BIOS zu deaktivieren. Sollte für die Aufgabenerfüllung ein Zugriff erforderlich sein, sind die PC-Benutzerinnen und PC- Benutzer schriftlich zu verpflichten, den Datenträger lediglich für diesen Zweck zu nutzen. Es ist dann zusätzlich durch mechanische Maßnahmen zu sichern (Fingerabdruck oder Passwort).

Externe Datenträger (z.B. USB-Anschlussmedien) sind vor ihrem Einsatz durch den EDV-Beauftragten auf vorhandenen schädigenden Code (z. B. Viren/Trojaner) zu prüfen.

Sollen dienstliche Daten auf externen Datenträgern gespeichert und weitergegeben werden, so sind die Datenträger zu prüfen, zu verschlüsseln und deren Nutzung zu überwachen. Dies verhindert einen Missbrauch der Daten durch dritte bei z.B. Verlust oder Diebstahl

Die Datenträger sind eindeutig zu kennzeichnen.

Nicht mehr benötigte Datenträger sind nach Rückgabe durch den Nutzer von dem EDV-Beauftragten unwiederbringlich zu löschen.

Der Anschluss von privaten Geräten an die dienstliche Infrastruktur ist nicht gestattet.

Benutzer/-innen - und Rechteverwaltung

Die Rechteverwaltung ist durch den EDV-Beauftragten wahrzunehmen.

Es ist eine bereichsbezogene Liste über PC-Benutzerinnen und PC-Benutzer und den ihnen zugewiesenen Rechten zu erstellen (Zugriffskonzept).

Benutzerinnen und Benutzer sind ausschließlich auf den Zentralservern (Domänencontroller über Active Directory) einzurichten.

Zur Vereinfachung der Rechtezuweisung sind Benutzergruppen zu bilden.

Den Benutzerinnen und Benutzern sind nur mit schriftlicher Zustimmung der jeweiligen Verfahrensverantwortlichen entsprechende Zugriffsrechte zu erteilen. Entsprechende Formulare sind vorhanden, eine E-Mail an die EDV-Abteilung ist als Nachweis ausreichend.

Die Berechtigungen sind soweit einzuschränken, dass ausschließlich verfahrensbezogene Speicher- oder Programmverzeichnisse genutzt werden können.

Letzte Änderung: 05.08.2021
Autor: Nico-Eugen Lange

SENIORENWOHNZENTRUM
VIADUKT

Sicherheitskonzept für die Internetnutzung

Der Seniorenwohnzentrum Viadukt GmbH

Allgemein

Der Leistungsumfang des Providers ist in einem ADV-Vertrag festzulegen. Es ist insbesondere darzustellen, auf welche Daten der Provider zugreifen kann.

Daten über den Ablauf der Internetkommunikation (z.B. Verlauf Proxyserver), die nicht für Abrechnungs- oder angeordnete Überwachungszwecke gespeichert werden, müssen unmittelbar nach Beendigung gelöscht werden.

Die Nutzung der Internetdienste ist in einer gesonderten Dienstanweisung zu regeln.

Die Befugnisse bzw. Zugriffsberechtigungen des EDV-Beauftragten sind festzulegen.

Die Administration der Internet-Komponenten ist zu protokollieren.

Veränderungen der Sicherheitseinstellungen sind nur mit Zustimmung der, durch die EDV-Abteilung durchzuführt

Die Überwachung der Internet-Kommunikation erfolgt durch unseren EDV-Beauftragten.

Sofern Dateien (z.B. Formulare u.a.) aus nicht vertrauenswürdigen Quellen oder unbekannten Internetseiten heruntergeladen werden, sind diese vor dem Öffnen einer Virenüberprüfung zu unterziehen. Das Herunterladen ausführbarer Programme und Dateien (Dateiendung: z. B. EXE, COM, BAT und VBS) ist auf den Arbeitsplätzen nur mit Zustimmung der EDV-Abteilung zugelassen, ggf. durch den Rechteentzug zu verhindern.

Physikalische Ebene

Die Übergänge vom internen Netz zum externen Netz sind durch Firewall-Systeme (z. B. Router, Gateways etc.) zu schützen.

Die Verbindung für die Internetdienste darf nur über die Leitung der Deutschen Telekom.

Die Verfügungsgewalt (Überwachung und Administration) über die eingesetzten Firewall-Komponenten (Router, Gateways etc.) im Bereich der Netzübergänge (intern/extern) liegt beim EDV-Beauftragten.

Es muss sichergestellt werden, dass Angriffe auf der physikalischen Ebene erkannt und abgewehrt werden.

E-Mail

E-Mail-Eingänge sind wie allgemeine Posteingänge zu behandeln.

Der E-Mail-Dienst ist über unseren Web Provider 1&1 Hosting (IONOS) abzuwickeln.

Für alle PC-Benutzerinnen und PC-Benutzer sind eindeutige E-Mail-Adressen vorzuhalten und/oder zusätzliche Funktions-E-Mail-Adressen einzurichten (z.B. Mahnungen, Datenschutz usw.)

E-Mails und die ihnen angehängten Attachments (Dateien), sind einer Virenüberprüfung zu unterziehen. Die dazu eingesetzte Virenschutzsoftware ist täglich zu aktualisieren.

Attachments mit ausführbaren Programmen und Dateien (Dateiendungen: z. B. EXE, COM, BAT und VBS) werden ohne weitere Überprüfung gelöscht.

Die Nutzung des dienstlichen E-Mail Accounts für private Mails ist nicht geduldet.

Die Nutzung eines Privaten E-Mail Accounts für geschäftliche Zwecke wird nicht geduldet.

E-Mails die an mehrere Personen extern verschickt werden, sind die Empfänger im Feld BCC einzutragen, bei internen Mails ist die Nutzung der BCC Funktion hingegen untersagt.

Beim Einrichten des Abwesenheitsassistenten ist darauf zu achten, dass keine Gründe für die Abwesenheit genannt werden.

In Einzelfällen muss bei länger andauerndem Ausfall wie z.B. Krankheit, der Zugriff auf die E-Mails des Abwesenden Mitarbeiters möglich sein, hierfür kann entweder der Mitarbeiter selbst oder im Zweifelsfall unsere IT eine Weiterleitung an die nächst zuständige Person oder eine Abwesenheitsnotiz eingerichtet werden, wie im Dokument "Arbeitsanweisung zu dem Datenschutz-konformen bearbeiten von E-Mails" zu finden.

Beim Versenden von E-Mails ist auf die Minimierung der personenbezogenen Daten zu achten, d.h. so wenig personenbezogene Daten wie möglich zu verwenden. Bei der Nutzung der Antwortfunktion auf eine eingehende E-Mail ist die ursprüngliche Nachricht zu entfernen. Bei einer Weiterleitung sind nicht für den Fall relevante Personenbezogene Daten zu entfernen.

Weitere Maßnahmen und Dienstanweisungen zur Nutzung von E-Mail Accounts und Bearbeitung unserer Einrichtung ersehen sie dem Dokument „Dienstanweisung zu dem Datenschutz-Konformen bearbeiten von E-Mails"

Homepage

Die Inhalte der Homepage sind mit dem Geschäftsführer und der Heimleitung abzustimmen.

Für die Darstellung personenbezogener Daten ist von den Betroffenen eine Einwilligung gemäß Art. 6 ff. DSGVO einzuholen.

Es muss sichergestellt werden, dass keine Manipulation der Daten durch Unbefugte möglich ist.

Die Integrität der Homepage ist in regelmäßigen Abständen zu überprüfen.

Die Homepage darf nur eine verschlüsselte Verbindung zulassen, um sicheren Kontakt z.B. über ein Formular zwischen Server und Benutzer zu gewährleisten. Diese Information ist in der Datenschutzerklärung zu erwähnen.

Werden auf der Homepage weitere Kommunikations- und Informationsmedien wie ein Newsletter angeboten, ist eine Nutzung dieses Services nur durch aktive Bestätigung der Datenschutzerklärung möglich (z.B. E-Mail Bestätigung)