Datenschutz Reglement

Wer	**Wann**	**Was**	**Version**
SIKNA Stiftung	April 2019	Dokument erstellt & implementiert	1.0
D. Homann (DSV)	Mai 2020	Ergänzt Videoreglement	1.1
J. Hanhart	Juli 2020	Revision durch Dipl. Datenschutz- & Informatiksicherheitsbeauftragter	1.1
RA R. Bloch	5. August 2020	Freigabe Dokument	1.1

Inhalt

1 Bedeutung, Ziel, Zugänglichkeit

(1) Dieses Datenschutzreglement ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten im Senioren Zentrum der SIKNA Stiftung. Ziel dieses Datenschutzreglements ist es, dass in der SIKNA Stiftung ein einheitlicher Datenschutzstandard gilt, welchem das Schweizer Datenschutzgesetz (nachfolgend „**DSG**“) zu Grunde liegt.

(2) Mit diesem Datenschutzreglement sollen die Grundrechte und Grundfreiheiten von Betroffenen, insbesondere ihr Recht auf Schutz personenbezogener Daten, gewahrt und geschützt werden.

(3) Dieses Datenschutzreglement muss für alle Beschäftigten und leitenden Angestellten jederzeit leicht zugänglich sein.

2 Geltungsbereich

(1) Dieses Datenschutzreglement findet Geltung auf das Senioren Zentrum der SIKNA Stiftung.

(2) Sie gilt persönlich für alle Beschäftigten und leitenden Angestellten der SIKNA Stiftung.

(3) Die Gebote und Verbote dieses Datenschutzreglements gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieser elektronisch oder in Papierform vonstattengeht. Ebenso beziehen sie alle Arten von Betroffenen (Bewohner, Beschäftigte, Lieferanten etc.) in ihren Geltungsbereich ein.

3 Begriffsbestimmungen

(1) Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (nachfolgend „Betroffener“). Bewohnerdaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name eines Ansprechpartners oder seine E-Mail-Adresse einen Rückschluss auf eine natürliche Person zu. Es genügt, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z.B. bei einer Mobilenummer. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.

(2) Besondere Arten oder Kategorien personenbezogener Daten sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

(3) Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(4) Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

(5) Profiling bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

(6) Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Massnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

(7) Anonymisierung ist die Verarbeitung von - grundsätzlich - personenbezogenen Daten in einer Weise, dass daraus der Personenbezug infolge Weglassens aller Identifikationsmerkmale durch niemanden (absolute Anonymisierung) oder nicht mehr mit vernünftigerweise zu erwartendem Aufwand (wieder-) herstellbar ist (faktische Anonymisierung).

(8) Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(9) Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des verantwortlichen verarbeitet.

(10) Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

(11) Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, ausser der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

(12) Eine Einwilligung des Betroffenen ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.

4 Datenschutzorganisation

(1) Der Stiftungsrat der SIKNA Stiftung trägt die oberste Verantwortung. Er beauftragt die Geschäftsleitung mit der Umsetzung des Datenschutzes innerhalb der SIKNA Stiftung. Die Geschäftsleitung bestellt keinen dedizierten Datenschutzbeauftragten, bezeichnet jedoch intern primär einen verantwortlichen Datenschutz für die die Umsetzung und Einhaltung der datenschutzrechtlichen Bestimmungen.

(2) Weiter wird eine Person als Datenschutzbeauftragter ernannt, welcher gegen innen wie aussen als erste

Anlaufstelle bei Fragen fungiert:

(2) Der verantwortliche Datenschutz überwacht die Einhaltung des DSG sowie anderer gesetzlichen Vorgaben, einschliesslich der Vorgaben dieser und anderer Richtlinien der SIKNA Stiftung zum Datenschutz.

(3) Die SIKNA Stiftung bzw. ihre Mitarbeiter haben den verantwortlichen Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen.

5 Umgang mit personenbezogenen Daten

(1) Die Verarbeitung personenbezogener Daten ist grundsätzlich untersagt, es sei denn, eine gesetzliche Norm erlaubt explizit den Datenumgang. Personenbezogene Daten dürfen nach dem DSG grundsätzlich verarbeitet werden:

- Bei einem bestehendes Vertragsverhältnis mit dem Betroffenen.
  Beispiel: Die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen eines Pflegevertrages mit einem Bewohner.
- Im Zuge vorvertraglicher Massnahmen auf Anfrage des Betroffenen sowie der Vertragsabwicklung mit dem Betroffenen.
  Beispiel: Bewohner B fordert Informationen zur Pflegedienstleistung P an und erwirbt dieses. Die erforderlichen Daten zur Zusendung des Informationsmaterials sowie zur Durchführung der Pflegeleistung dürfen verarbeitet werden.
- Im Rahmen der Verarbeitung von personenbezogenen Daten von Bewerbern und Mitarbeitenden.
- Wenn und soweit der Betroffene eingewilligt hat.
  Beispiel: Der Betroffene meldet sich zu einem Anlass an.
- Wenn eine rechtliche Verpflichtung besteht, der die SIKNA Stiftung unterliegt.
  Beispiel: Gesetzliche Aufbewahrungsfristen.
- Wenn berechtigte Interessen der SIKNA Stiftung bestehen, sofern nicht die Interessen oder Grundrechte des Betroffenen überwiegen.
  Beispiel: Die Nutzung der postalischen Anschrift zur Aussendung von Werbeschreiben.

Bei Fragen und Unsicherheiten ist der Datenschutzbeauftragte vorgängig zu konsultieren.

(2) Betroffene dürfen nur unter bestimmten Voraussetzungen einer ausschliesslich auf einer automatisierten Verarbeitung – so auch dem Profiling – beruhenden Entscheidung unterworfen werden, die ihnen gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Der verantwortliche Datenschutz ist vor Einführung solcher automatischen Verarbeitungen zu konsultieren.

(3) Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. Eine Datenhaltung ohne Zweck, so beispielsweise die Speicherung von Daten auf Vorrat, ist unzulässig.

(4) Falls möglich sollte auf einen personenbezogenen Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen.

(5) Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist – neben der erklärten Einwilligung durch den Betroffenen – nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist. Hierbei sind insbesondere die vernünftigen Erwartungen des Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegenüber dem Unternehmen, die Art der verwendeten Daten, die Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu berücksichtigen.

(6) Der Betroffene ist bei der Erhebung seiner personenbezogenen Daten umfassend über den Umgang mit seinen Daten zu informieren. Bewohner sind deshalb auf die im Internet publizierte und beim Empfang erhältliche Datenverarbeitungsgrundsätze hinzuweisen (Datenschutzerklärung für Bewohner).

(7) Werden personenbezogene Daten nicht beim Betroffenen erhoben, sondern beispielsweise von einem anderen Heim beschafft, ist der Betroffene grundsätzlich nachträglich und umfassend über den Umgang mit seinen Daten informieren. Zudem muss über eine (spätere) Änderung der Ziel- und Zweckbestimmung der Datenverarbeitung vor der Weiterverarbeitung informiert werden. In Fällen gemäss diesem Abschnitt ist der Datenschutzbeauftragte vorgängig zu konsultieren.

(8) Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf dem neusten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die jeweilige Fachabteilung hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmässig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen. Gesetzliche, regulatorische oder betrieblich definierte Archivierungsvorschriften sind jedoch einzuhalten. Bei Fragen und Unsicherheiten ist der Datenschutzbeauftragte zu konsultieren.

6 Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogene Daten (wie Gesundheitsdaten) dürfen grundsätzlich vom Betroffenen erhoben, verarbeitet oder genutzt werden, wenn der Betroffene über

(1) den Inhalt der Datensammlung,
(2) dem Zweck der Datenbearbeitung und
(3) die Kategorien der Datenempfänger informiert worden ist.

Diese Anforderung ist grundsätzlich erfüllt, wenn z.B. einem Bewohner die Datenschutzerklärung für Bewohner bzw. deren Vertreter bekannt ist. Ferner sind zusätzliche technische und organisatorische Massnahmen (z.B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

7 Datenübermittlung

(1) Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund vertraglicher, gesetzlicher oder regulatorischer Notwendigkeit oder der Einwilligung des Betroffenen zulässig.

(2) Befindet sich der Empfänger personenbezogener Daten ausserhalb der schweizerischen Eidgenossenschaft oder des Europäischen Wirtschaftsraums, bedarf es in den meisten Fällen besonderer Massnahmen zur Wahrung von Rechten und Interessen Betroffener (z.B. durch Sicherstellung eines angemessenen Datenschutzniveaus).

(3) Bei Fragen und Unsicherheiten zu jeder Art der Übermittlung ist der Datenschutzbeauftragte vorgängig zu konsultieren.

8 Externe Dienstleister

(1) Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der Datenschutzbeauftragte vorab zu informieren.

(2) Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
- Technisch-organisatorische Sicherheitsmassnahmen
- Erfahrung des Anbieters im Markt
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schliessen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.)

(3) Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung, der erhöhten Anforderungen genügen muss. Der verantwortliche Datenschutzbeauftragte ist beizuziehen.

(4) Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Massnahmen regelmässig zu überprüfen. Das Ergebnis ist zu dokumentieren.

9 Datenminimierung, Privacy by Design / Privacy by Default

(1) Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einem Betroffenen zu erheben, zu verarbeiten oder zu nutzen („Datenminimierung“). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist. Beispielsweise wird es im Rahmen einer statistischen Auswertung von Daten nicht notwendig sein, den vollen Namen eines Betroffenen zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrundeliegenden Information ebenfalls gewährleisten kann.

(2) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen („Privacy by Design/Privacy by Default“). Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern, so insbesondere den Grundsatz der Datenminimierung.

10 Rechte von Betroffenen

(1) Unter Betroffenenrechten im Datenschutz versteht man die Rechte einer von einer Datenverarbeitung betroffenen Person gegenüber dem Verantwortlichen. Die umfassenden Betroffenenrechte bringen Pflichten mit sich, denen das Unternehmen nachkommen muss. Hierunten fallen nicht nur Informationspflichten, sondern auch Auskunfts- und Meldepflichten, welche ohne ausreichende Informationstransparenz nicht erfüllt werden können. Zu den Rechten der Betroffenen gehören ein Recht auf Auskunft, Berichtigung und Vervollständigung, ein Recht auf Löschung („Vergessenwerden“) und Einschränkung (inkl. Sperrung), ein Widerspruchsrecht sowie das Recht auf Datenübertragbarkeit.

(2) Nimmt ein Betroffener insbesondere sein Recht auf Auskunft, sein Anspruch auf Berichtigung, sein Recht auf Löschung oder sein Recht auf Einschränkung wahr, ist umgehend der verantwortliche Datenschutz einzubeziehen, da solchen Anträgen grundsätzlich innert 30 Tagen nachzukommen ist – wenn nicht bessere Rechte der SIKNA Stiftung dem entgegenstehen. Der rechtzeitige Beizug des Datenschutzbeauftragten ist empfohlen.

11 Auskunftsersuchen Dritter über Betroffene

(1) Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise Bewohner oder Beschäftigte der SIKNA Stiftung, ist eine Weitergabe von Informationen nur zulässig nach vorgängiger Rücksprache mit dem Datenschutzbeauftragten und allenfalls dem Betroffenen.

12 Verzeichnis von Verarbeitungstätigkeiten

(1) Das Unternehmen hat ein Verzeichnis über alle Datenverarbeitungen

(1) mit besonders schützenswerten Daten (insbesondere mit Gesundheitsdaten) und

(2) bei welchen regelmässig Personendaten an Dritte bekannt gegeben werden,

zu führen. Die Standards für das Verzeichnis legt die Geschäftsleitung fest. Der Datenschutzbeauftragte kann zur Beratung hinsichtlich der gesetzlich geforderten Informationen hinzugezogen werden. Diese Datensammlungen sind dem Beauftragten des Bundes zu melden, soweit keine gesetzliche Verpflichtung zur Bearbeitung besteht.

(2) Der verantwortliche Datenschutz hält in der Regel einmal jährlich mit den Abteilungen hinsichtlich Änderungen und oder Ergänzungen Rücksprache.

(3) Die SIKNA Stiftung stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Zuständig hierfür ist der verantwortliche Datenschutz nach vorgängiger Rücksprache mit dem Datenschutzbeauftragten und der Geschäftsleitung.

13 Werbung

(1) Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat. Das umfasst auch den Versand von Newslettern, welcher zwingend unter Beizug der Marketingabteilung zu erfolgen hat.

(2) Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig. Bitte konsultieren Sie diesbezüglich den Datenschutzbeauftragten.

14 Schulung

Beschäftigte, die ständig oder regelmässig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Die Geschäftsleitung entscheidet verbindlich über Form, Turnus und erforderliche Teilnehmer der entsprechenden Schulungen. Teilnahme und allfällige Testresultate sind zu dokumentieren.

15 Beschwerden

(1) Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstösse gegen dieses Datenschutzreglement jederzeit anzeigen.

(2) Die zuständige Stelle für die oben genannten Beschwerden ist der verantwortliche Datenschutz, welcher den Datenschutzbeauftragten beizieht.

16 Audits

(1) Um ein hohes Datenschutzniveau zu gewährleisten, können relevante Prozesse durch Audits interner Stellen oder durch externe Auditoren überprüft werden. Im Falle der Feststellung eines Verbesserungspotentials sind unmittelbare Abhilfemassnahmen zu treffen.

(2) Die beim Audit gewonnenen Erkenntnisse sind zu dokumentieren und mit den verantwortlichen Mitarbeitern zu diskutieren.

(3) Ein Audit ist erfolgreich abgeschlossen, wenn alle im Bericht dokumentierten Massnahmen umgesetzt sind. Bei Bedarf können Follow-up-Audits durchgeführt werden, indem Empfehlungen des initialen Audits einer Überprüfung ihrer Implementierung unterzogen werden.

17 Interne Ermittlungen

(1) Massnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere muss die damit einhergehende Datenerhebung und -verwendung zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen des Betroffenen verhältnismässig sein. Die Einsichtnahme in schriftliche wie elektronische Korrespondenz von Mitarbeitern ist erlaubt, soweit erhebliche Verstösse gegen Gesetz, Regulatorien oder arbeitsvertragliche Pflichten vermutet werden und der Eingriff verhältnismässig erfolgt. Solche Untersuchungen sind vorgängig vom Stiftungsrat oder vom Geschäftsführer genehmigen zu lassen.

(2) Der Betroffene ist so bald wie möglich über die zu seiner Person durchgeführten Massnahmen zu informieren.

(3) Bei allen Formen der internen Ermittlungen ist der Datenschutzbeauftragte hinsichtlich der Auswahl und Ausgestaltung der Massnahmen vorab einzubeziehen.

18 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

(1) Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird in Zusammenarbeit mit dem IT-Provider ein allgemeines Sicherheitskonzept in Abhängigkeit der Schutzbedarfsfeststellung und Risikoanalyse erstellt, das für alle Verfahren verbindlich ist. Hierin ist insbesondere der Stand der Technik ebenso zu berücksichtigen, wie Mittel und Massnahmen zur Verschlüsselung und Datensicherung. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Massnahmen regelmässig zu überprüfen, zu bewerten und zu evaluieren.

(2) Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Türen unbesetzter Räume sind zu verschliessen. Wirksame Massnahmen zur Zugangskontrolle an Geräten müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit stets zu sperren.

(3) Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden.

(4) Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-to-know-Prinzip“). Zugriffsberechtigungen müssen festgelegt und dokumentiert sein.

(5) Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln bzw. zu anonymisieren. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

19 Verletzungen des Schutzes von Daten („Datenpanne“)

(1) Sollten Stiftungsdaten unrechtmässig Dritten offenbart worden sein, sind folgende Personen unverzüglich (innert 6 Stunden) zu informieren:

- Geschäftsleitung
- verantwortlicher Datenschutz
- Datenschutzbeauftragter

Sie erarbeiten die Sachverhaltsaufklärung gemeinsam.

(2) Diese erste Meldung hat möglichst alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen; insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

(3) Die Erfüllung einer etwaigen Informationspflicht gegenüber der Aufsichtsbehörde erfolgt ausschliesslich durch die Geschäftsleitung. Betroffene können nach Wahl der Geschäftsleitung durch diese selbst, durch den von der Geschäftsleitung bestimmte Person informiert werden.

20 Folgen von Verstössen

Ein fahrlässiger oder gar mutwilliger Verstoss gegen dieses Datenschutzreglement kann arbeitsrechtliche Massnahmen nach sich ziehen, einschliesslich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

21 Videoüberwachung

Die SIKNA Stiftung betreibt, gestützt auf Art. 328 OR & Bundesgesetz über den Datenschutz (DSG) ein Videoüberwachungssystem mit Kameras. Die Handhabung des Systems und die Standorte der Kameras sind dem Videoreglement SIKNA Stiftung Zürich, aktuelle Version zu entnehmen. Die jeweils gültige Version kann von berechtigten Personen jederzeit am Empfang des Senioren Zentrums eingesehen werden.

Version: Datenschutzreglement 05/2020

In Kraft seit April 2019, ergänzt Mai 2020